NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ENTERING THE MATRIX: THE CHALLENGE OF REGULATING RADICAL LEVELING TECHNOLOGIES

by

Jennifer J. Snow

December 2015

Thesis Advisor: Leo J. Blanken
Co-Advisor: Zachary S. Davis

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average one hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2015	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE ENTERING THE MATRIX: THE CHALLENGE OF REGULATING RADICAL LEVELING TECHNOLOGIES			**5. FUNDING NUMBERS**
6. AUTHOR(S) Jennifer J. Snow			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Lawrence Livermore National Laboratory 7000 East Avenue • Livermore, CA 94550			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the US government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE** A

13. ABSTRACT

Radical Leveling Technologies (RLT) constitute a new class of technologies that have exponential disruptive effects across a diverse set of societal processes resulting in radical change. This emerging class has profound leveling effects. Users can leverage RLT to produce national or international impacts without the need for significant technological expertise. These effects may occur via digital diffusion and without the need for extensive infrastructure. RLT are being driven by the power and expertise of online Open Source Communities. The ability of existing policy and enforcement methods to regulate this class of technology successfully, particularly within the counterproliferation space, suggests that a paradigm change is necessary. A spectrum of potential solutions is considered which advocates for collaborative efforts vice "hard policing" measures to engage online communities while also providing options to build additional security capacity within the government and law enforcement communities. Capacity can be gained via unconventional means including the use of cyber bounties, cyber privateering, hybrid fusion centers, and decentralized autonomous technology teams to improve support to existing special operations efforts, particularly within the counterproliferation mission set.

14. SUBJECT TERMS Radical Leveling Technologies, additive manufacturing, synthetic biology, biohacking, 3D printing, emerging disruptive technology, technology regulation, technology policy, technology convergence, counterproliferation, counterterrorism, interagency collaboration	**15. NUMBER OF PAGES** 131
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

ENTERING THE MATRIX: THE CHALLENGE OF REGULATING RADICAL LEVELING TECHNOLOGIES

Jennifer J. Snow
Major, United States Air Force
B.S., Salisbury University, 1996
B.S., University of Maryland Eastern Shore, 1996
B.A., Salisbury University, 2001
M.A., American Military University, 2008

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
December 2015

Approved by: Leo J. Blanken
Thesis Advisor

Zachary S. Davis
Co-Advisor

Dr. John Arquilla
Chair, Defense Analysis Department

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Radical Leveling Technologies (RLT) constitute a new class of technologies that have exponential disruptive effects across a diverse set of societal processes resulting in radical change. This emerging class has profound leveling effects. Users can leverage RLT to produce national or international impacts without the need for significant technological expertise. These effects may occur via digital diffusion and without the need for extensive infrastructure. RLT are being driven by the power and expertise of online Open Source Communities. The ability of existing policy and enforcement methods to regulate this class of technology successfully, particularly within the counterproliferation space, suggests that a paradigm change is necessary. A spectrum of potential solutions is considered which advocates for collaborative efforts vice "hard policing" measures to engage online communities while also providing options to build additional security capacity within the government and law enforcement communities. Capacity can be gained via unconventional means including the use of cyber bounties, cyber privateering, hybrid fusion centers, and decentralized autonomous technology teams to improve support to existing special operations efforts, particularly within the counterproliferation mission set.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1

A. RISE OF THE RLT: EXPONENTIAL VS. LINEAR TECHNOLOGY....4

B. PURPOSE....6

C. RESEARCH QUESTIONS....7

D. APPROACH....8

E. ORGANIZATION....9

II. DEFINING THE RLT....11

A. RLT DEFINED: CHARACTERISTICS OF THE CLASS....12

B. ADDITIVE MANUFACTURING: THE EVOLUTION OF AN RLT....13

C. OPEN-SOURCE COMMUNITIES: DRIVERS OF EXPONENTIAL CHANGE....17

III. CHALLENGES POSED BY RLT....25

A. ENABLING FACTORS....26

B. RLT THREAT VECTORS: THE SHAPE OF THINGS TO COME....28

C. ASIA, RLT, AND THE COUNTERPROLIFERATION PROBLEM....29

D. WHEN PROLIFERATION GOES DIGITAL....30

E. SYNTHETIC BIOLOGY AND BIOHACKING: ENABLING EXPONENTIAL PROMISE, REGULATING EXPONENTIAL THREATS....33

F. UNDERSTANDING THE REGULATORY GAPS....36

G. CONVERGENCE: THE EFFECTS OF EXPONENTIAL TECHNOLOGY SQUARED....37

H. THE NEED FOR A NEW PARADIGM....41

IV. NAVIGATING THE COMPLEX CULTURE DRIVING RADICAL LEVELING TECHNOLOGIES....43

A. *MGM V. GROKSTER*: THE PEER-TO-PEER PROBLEM....49

B. THE CYPHER WAR PERIOD: ZIMMERMAN, BERNSTEIN, AND JUNGER VS. US POLICY....52

C. POLICY PITFALLS: PHILADELPHIA'S 3D GUN BAN....57

D. LIGHTSQUARED: TECHNOLOGY VS. THE GOVERNMENT....59

E. THE FBI AND BIOHACKING: BUILDING A CULTURE OF SHARED SECURITY VALUES 62
F. THE BATTLE FOR CRITICAL INFRASTRUCTURE SECURITY: DHS AND ICS-CERT 65
G. FINEST SQUAD: HACKERS DEFEATING BOT-THUGS WITH CYBER SELF-POLICING 68
H. HACKTIVISM: HOW GROUPS LIKE ANONYMOUS ARE HELPING TO IMPROVE SECURITY 69
I. EXPONENTIAL EFFECTS OF DIGITAL PARTNERS: DHS AND THE SD-LECC MODEL 71

V. A FLEXIBLE SPECTRUM FOR END-GAME SUCCESS 75
A. POLICY PITFALLS AND FAILED DETERRENCE 76
B. MOVING FORWARD TO THE FUTURE: A SPECTRUM OF SOLUTIONS 78
C. COLLABORATIVE EFFECTS 79
D. REGULATORY EFFECTS 81
E. ACTIVE EFFECTS 82
F. OFFENSIVE EFFECTS 85

VI. CONCLUSIONS AND ADDITIONAL RESEARCH RECOMMENDATIONS 87

LIST OF REFERENCES 91

INITIAL DISTRIBUTION LIST 113

LIST OF FIGURES

Figure 1. Additive Manufacturing: An Example of RLT Effects 6
Figure 2. 3D Printing Impacts 16
Figure 3. Spectrum of Solutions 79

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Traditional Regulation of 3D-Printing Digital Design 55

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AM	Additive Manufacturing
BAB	BioAssemblyBot
CSC	Computer Sciences Corporation
DATT	Decentralized Autonomous Technology Teams
DDos	denial of service
DHS	Department of Homeland Security
DIY	do-it-yourself
DNA	deoxyribonucleic acid
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IDA	Infocomm Development Authority
IMA	InfraGard Members Alliance
INMA	InfraGard National Members Alliance
IRL	in real life
IS	Islamic State
ISIS	Islamic State in Iraq and Syria
ITAR	International Traffic in Arms Regulations
JCVI	J. Craig Venter Institute
OSC	Open Source Community
P2P	peer-to-peer
PGP	Pretty Good Privacy
RLT	Radical Leveling Technology
SD-LECC	San Diego Law Enforcement Coordination Center
TSIM	Tissue Structure Information Modeling
UL	Underwriters Laboratory
USML	U.S. Munitions List
VPN	Virtual Private Network
WMD	weapon of mass destruction

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Special thanks to my thesis advisors, Dr. Leo Blanken and Dr. Zack Davis, for their mentorship and advice during this process and to the Fantastic Four, Derek, Kai, Matt, and Matt, for allowing me to play a role in their efforts to make the world a safer place.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

On June 26, 2015, authorities in Hong Kong arrested nine members of a terrorist cell who were believed to be planning a series of attacks on government buildings meant to disrupt upcoming elections. When the group was arrested, officials discovered a stack of pellet air guns, explosives, and a 3D printer. It was unclear how the group intended to use the 3D printer in their plot. Producing modified toy guns that function as real weapons or creating parts for specialized explosive devices were just two of the many possibilities.

The most important takeaway from this event is how rapidly security policy and enforcement are falling behind criminal adoption of advanced technologies.[1] A new class of emerging technologies is creating significant gaps between policy, regulation, and reality across a diverse range of areas. Three-dimensional printing, also known as additive manufacturing (AM) or the process of turning digital design into physical objects is one such example. In 2012, Glasgow University chemist Lee Cronin turned a 3D printer into a pharmaceutical-grade chemical production computer that would allow individuals to manufacture their own prescription drugs using chemical recipes posted on the Internet. In 2015, Germany produced the first 3D printer specifically designed for drug production and the Food and Drug Administration (FDA) approved the first 3D-printed drugs for use in the United States.[2] While the benefits of such innovation are undeniable, the world of illicit narcotics suddenly became much more complicated for

[1] Heidi Milkert, "Hong Kong Terrorists Caught with 3D Printer, Perhaps Looking to Modify Airsoft Guns," *3DPrint.com*, June 26, 2015, http://3dprint.com/76737/3d-printer-terrorists/; Marc Goodman, "Crime Has Gone High-Tech, and the Law Can't Keep Up," *Wired*, March 21, 2015, 1–2.

[2] Eddie Krassenstein, "German Company Aims to Sell 3D Printed Drugs & A 3D Drug Printer." *3DPrint.com*, August 10, 2015; Susan Scutti, "FDA Approves First Ever 3D-Printed Epilepsy Drug from Aprecia; Set to Create More Central Nervous System Pills," *Medical Daily*, August 4, 2015; David B. Samadi, "You Can Now 3D Print Prescription Drugs," *Observer*, August 12, 2015, http://observer.com/2015/08/print-your-prescription-3d-technology-modernizes-medicine/; Dominic Basulto, "Why it Matters That the FDA Just Approved the First 3D-Printed Drug," *Washington Post*, August 11, 2015. https://www.washingtonpost.com/news/innovations/wp/2015/08/11/why-it-matters-that-the-fda-just-approved-the-first-3d-printed-drug/.

regulators and policymakers.[3] In 2014, Andrew Hessel, a cell biologist and geneticist working for 3D-printing giant Autodesk, claimed that he was printing deoxyribonucleic acid (DNA) and had created viruses to combat cancer. The process took two weeks and cost $1,000. These techniques, if successful, will revolutionize the pharmaceutical and medical communities.[4] Craig Venter, whose institute created the first synthetic life-form, is also pursuing 3D printing as a way to design vaccines that can be produced and shared globally in under twenty-four hours. Even amateur labs and biohackers (biology and chemistry hobby groups who seek simple solutions to global science challenges) will soon be able to join the 3D-printed biological revolution. It is because of these spaces that security experts and professionals like Dr. Venter have concerns. Fears that such groups may be exploited by bad actors who seek to advance their own threat capabilities are accompanied by the concern that individuals participating in these groups may produce threats inadvertently due to ignorant experimentation. The public now has easy access to tools that allow anyone, even those with no scientific background, to manipulate and create with genetic materials. More alarming still is that the use of such technologies may critically change the security environment and the way in which future wars will be fought by both states and non-state actors.[5]

Much of this innovation is occurring in public spaces or online forums, driven by a global community of open-source entities who come together voluntarily to work on global problems. These "do-it-yourself" (DIY) communities are enabling the exponential

[3] Stephen Kotler, "Vice Wars: How 3-D Printing Will Revolutionize Crime," *Forbes*, July 13 2012, http://www.forbes.com/sites/stevenkotler/2012/07/31/the-democratization-of-vice-the-impact-of-exponential-technology-on-illicit-trades-and-organized-crime/.

[4] Katie Collins, "Meet the Biologist Hacking 3D Printed Cancer-Fighting Viruses," *Wired UK*, October 16 2014.

[5] Harry Bentham, "Virus: Rebutting the Fear of Synthetic Biology," Institute for Ethics and Emerging Technologies, May 13, 2014.

advancement of technologies like 3D printing which are rapidly outpacing national-government and international-organization regulatory and intelligence capacities.[6]

The above examples provide a simple demonstration of how technology is challenging security experts on multiple fronts. This thesis will discuss technologies that, when combined with the power of Open Source Communities (OSCs), create the ability for non-state actors or even individuals to gain access to new forms of power that can rival that of a nation-state or can be shared globally via the Internet to empower others around the world.[7] In other words, we will be looking at jointly sufficient conditions for a "radical leveling effect." These conditions are 1) the technology is disruptive (a game changer), 2) the Internet allows it to be diffused in part or entirely via digital transmission, and 3) there is very little or no infrastructure or large-scale investment necessary to facilitate it. If any of these conditions are not met, then the technology will not have radical leveling effects as exhibited by the Radical Leveling Technology (RLT) class as a whole.

In order to focus the discussion, 3D printing or additive manufacturing (AM) will be used as the primary representative of this class of technologies. Where appropriate, other RLT such as synthetic biology, neurotechnology or the internet will be highlighted to illustrate specific points, and the convergence of these technologies will be discussed to showcase disruptive effects and provide policymakers with an understanding of the

[6] Shane Coughlan, ed., *Research on Open Innovation: A Collection of Papers on Open Innovation from Leading Researchers in the Field* (N.p: OpenForum Europe, 2014); Libby Clark, "Jono Bacon: Open Source is Where Society Innovates," *Linux.com*, October 14, 2014, https://www.linux.com/news/featured-blogs/200-libby-clark/791644-jono-bacon-open-source-is-where-society-innovates; Chiara Franzoni and Henry Sauermann, "Crowd Science: The Organization of Scientific Research in Open Collaborative Projects," *Research Policy* 43, no. 1 (2014): 1–20, doi: 10.2139/ssrn.2167538; Jack M. Germain, "Next on the Open Source Horizon: 3D Printing," *LinuxInsider*, May 28, 2014, http://www.linuxinsider.com/story/80519.html; Nozomi Hayase, "Blockchain Revolution: Open Source Democracy for the 99%," *openDemocracy UK*, August 4, 2014, https://www.opendemocracy.net/ourkingdom/nozomi-hayase/blockchain-revolution-open-source-democracy-for-99; Eric Raymond, *The Cathedral & the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*, 3rd ed. (Sebastopol, CA: O'Reilly, 2001); Robert David Steele, *The Open-Source Everything Manifesto; Transparency, Truth & Trust* (Berkeley, CA: Evolver, 2012).

[7] Tim Bajarin, "This Will Be the Most Disruptive Technology over the Next Five Years," *Time*, January 12, 2015, 1–3, http://time.com/3663909/technology-disruptive-impact/; Jeremy Heimans, "What New Power Looks Like," TED video, 15:08, June 2014, https://www.ted.com/talks/jeremy_heimans_what_new_power_looks_like?language=en; Clay Shirky, "How the Internet Will (One Day) Transform Government," TED video, 18:32, June 2012, https://www.ted.com/talks/clay_shirky_how_the_internet_will_one_day_transform_government?language=en.

challenges to come. This chapter begins with a brief look at the development and evolution of these technologies, starting with the difference between traditional technologies and Radical Leveling Technology (RLT). The five core questions that drove this thesis are introduced, along with the case-study methodology. The chapter concludes with an overview of the remaining chapters. While the intent of this thesis is to provide a starting point for understanding RLT and some initial options to prevent dangerous use of such technology, it still aims to provide a broad perspective on RLT. Emphasis is placed on the need to develop in-depth expertise on RLT in order to construct a strategy to address the challenges posed by this technology class. Policy and regulation in this area, if done ignorantly and in a reactive fashion, will function to make the state and the public less secure. Some of this damage may have effects from which there is no option for recovery. The brave new world of nascent RLT may be forgiving now, but in a few years, the security landscape is going to change dramatically. At that point, if policymakers are not ready to face these challenges, the state will suffer diplomatically, militarily, and economically. This thesis is the first step on the path to preventing that from happening.

A. RISE OF THE RLT: EXPONENTIAL VS. LINEAR TECHNOLOGY

When Martin Cooper, an engineer working for Motorola, made a call on the first cell phone in 1973, no one could have predicted the evolution that was to follow.[8] Much like the personal computer, the cell phone evolved slowly for ten years before the first handheld became commercially available, and then it was another ten years before this technology was accessible to the general public. If Martin back in 1973 had announced that in forty years cell phones would become smartphones on which text messages and emails could be sent and photos and videos could be shared, that people would be able to shop and bank from these devices, unlock their cars, play music, or even remotely set the temperatures on their thermostats, many would have dismissed this as sheer fantasy, the stuff of science fiction. Certainly no one foresaw cell phones being used as triggers for

[8] Nicole Nguyen, "The Evolution of the Cell Phone—How Far It's Come!" *ReadWrite*, July 4, 2014, http://readwrite.com/2014/07/04/cell-phone-evolution-popsugar.

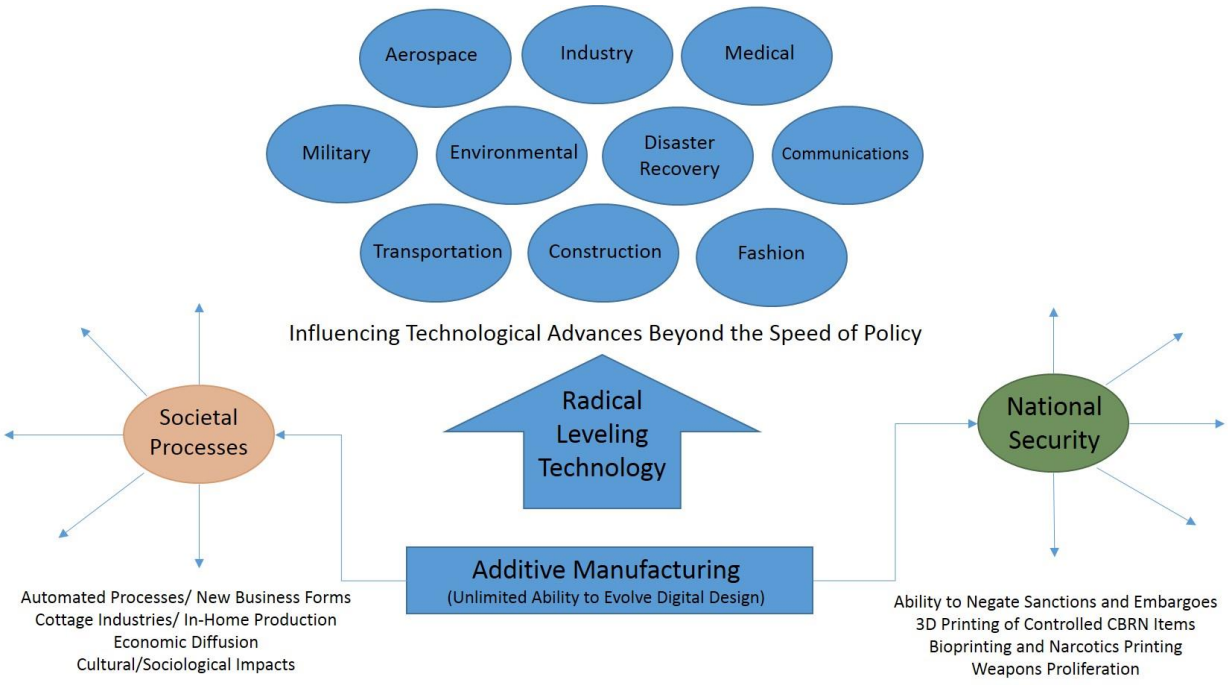
explosive devices or as tools for identity theft. And yet not only does this technology exist but it continues to evolve and shape communications culture and technology.[9]

The evolutions of the cell phone, the personal computer, video game consoles, eight-track tapes to CD, and VCR to Blu-ray player are all disruptions. However, while these technologies enhanced aspects of society, their primary impacts were in the areas they were designed for—communications, audio/visual applications, entertainment, or information technology. They only served to disrupt and replace the technology within those defined spaces. This process is what many have come to expect as normal for technological evolutions: predominately linear, with perhaps a few branches (e.g., tablet devices, touchscreens, and digital readers or the addition of video and photography capabilities to our handheld devices) and a few unexpected developments (e.g., branchless banking, geolocation capabilities, and bomb making) that still fall predominately within existing legal and regulatory parameters. But this predictable pattern of technological evolution has started to change in a big way.

Today, a new species of emerging technologies is looming. Born of the Internet, maintaining one foot in cyber with the ability to manifest physical impacts, both disruptive and transformative, to multiple technologies as well as existing societal processes and with the ability to provide non-state actors with technology that can enable them to rival nation-state power, RLT present a raw challenge, one that will require a new approach to national security policy and regulatory efforts.

[9] Alexander Trowbridge, "Evolution of the Phone: From the First Call to the Next Frontier," *CBS News*, December 6, 2014, http://www.cbsnews.com/news/evolution-of-the-phone-from-the-first-call-to-the-next-frontier/.

Figure 1. Additive Manufacturing: An Example of RLT Effects



B. PURPOSE

Due to the persistent innovation enabled by the Internet, non-state actors are gaining access to technologies that allow them to achieve parity at the state and regional governance levels. Groups like Hezbollah, Hamas, and Islamic State are able to use technology as non-state actors to exploit the Westphalian state-centric system to their advantage. These technologies are changing the balance of power, creating a world in which a small group can address heads of state or a group such as Hezbollah can leverage technology to militarily compete with Israel.[10] As technological development continues

[10] Emily O. Goldman and Leo J. Blanken, "The Economic Foundations of Military Power," in *Guns and Butter: The Political Economy of International Security,* ed. Peter Dombroski. (Boulder, CO: Lynne Rienner, 2005), 37; Daniel Siryoti, "Iran Admits Hezbollah's Drone over Israel Used Iranian Technology," *Associated Press*, October 14, 2012, http://www.israelhayom.com/site/newsletter_article.php?id=6075; Yochi Dreazen, "The Next Arab-Israeli War Will Be Fought with Drones," *Diplomat*, March 26 2014; Marc Goodman and Parag Khanna, "The Power of Moore's Law in a World of Geotechnology," *National Interest* no. 123 (January-February 2013): 64–73; Amy Zegart, "The Coming Revolution of Drone Warfare," *Wall Street Journal*, March 18, 2015, http://www.wsj.com/articles/amy-zegart-the-coming-revolution-of-drone-warfare-1426720364.

rapidly, it is imperative that nation-states and international security organizations devise effective legal and regulatory responses to address the changing balance of power and the potential for proliferation of advanced, hard to detect, easy to produce, easy to proliferate threat technologies that can create national or regional impacts.[11]

This thesis will explore RLT and then conduct a qualitative analysis on one example: additive manufacturing (commonly referred to as 3D printing). AM was chosen due to its accessibility, familiarity among the public and because it is currently center stage in several policy and regulatory discussions. The reader will be exposed to the unique security challenges posed by RLT and shown a comparative case-study review that highlights both successful and failed tactics in dealing with specific aspects of these technologies. Discussion of a flexible spectrum of solutions that can be employed and evolved to address current and future RLT will be included.

C. RESEARCH QUESTIONS

Upon completion of an initial literature review, five key research questions were identified as core to the discussion on RLT. The first two are concerned with how non-state actors and rogue states may seek to leverage RLT and the degree to which they might gain nuclear parity with nation-states. More specifically, this section focuses on understanding the capabilities and limitations of these technologies within the security and law-enforcement arenas. The third question concerns the possible ways for the US government and its allies to receive advance warning of potential threats to civilian international security, examining the need to understand the culture driving these

[11] W. McLaughlin, "The Use of the Internet for Political Action by Non-State Dissident Actors in the Middle East," *First Monday* 8, no. 11 (November 2003), doi: 10.5210/fm.v8i11.1096; Conner M. McNulty, Neyla Arnas, and Thomas Campbell, "Toward the Printed World: Additive Manufacturing and Implications for National Security," *Defense Horizons*, no. 73 (September 2012): 1–16; Gerald Walther, "Printing Insecurity? The Security Implications of 3D-Printing of Weapons," *Science and Engineering Ethics* (December 2014): 1–11, doi: 10.1007/s11948-014-9617-x; Jillian York, "EFF Signs Joint Coalition Letter Urging Companies to be Proactive on Export Regulations," Electronic Frontier Foundation, June 27, 2012, https://www.eff.org/deeplinks/2012/06/eff-signs-joint-coalition-letter-urging-companies-be-proactive-export-regulations; Nick Thorpe, "Hungary Internet Tax Cancelled after Mass Protests," *BBC News*, October, 31, 2014, http://www.bbc.com/news/world-europe-29846285?print=true; Zeynep Tufekci and Christopher Wilson, "Social Media and the Decision to Participate in Political Protest: Observations from Tahrir Square," *Journal of Communication* 62, no. 2 (April 2012): 363–79, doi: 10.1111/j.1460-2466.2012.01629.x; US Department of State, "Controls Tangible/Intangible," accessed January 8, 2015, http://www.state.gov/strategictrade/practices/c43180.htm.

technologies as well as effective alternatives that will aid in addressing informational gaps. The final two questions look at the degree to which RLT may be susceptible to law enforcement and regulation and the need to balance security against potential benefits such technology may bring to societies. This discussion seeks to establish a foundational framework from which the law enforcement and national security communities can stay current on evolutions in RLT and ensure that government efforts are not outpaced by future evolutions.

D. APPROACH

This thesis focuses on AM as an example of the many RLT developing from the open-source innovation of the Internet today. The selection of AM was appropriate because it is the most publicly familiar and the most easily translated. In addition, AM displays all of the features of a typical RLT including a radically transformative, disruptive nature that will usher in the next generation of existing technologies and societal processes.

Since AM and other RLT have just recently come to the forefront of public consciousness, the body of knowledge on how to approach security concerns and regulation within the digital environment is still fairly immature. A series of cross-sectional case studies representative of failed and successful interactions between government, corporate, and regulatory entities and the online OSCs that are the drivers behind the majority of RLT will be examined to glean the necessary characteristics for a successful spectrum of solutions that policymakers and regulators can apply to current and future RLT. This foundation should provide an approach that can then be evolved in

tandem with technological changes to control diffusion and deter the development of technological threat vectors useful to non-state actors and rogue states.[12]

E. ORGANIZATION

This thesis is organized into five chapters, beginning with the definition of the RLT species and ending with recommendations on a way forward. The second chapter introduces RLT and AM and shows the tremendous potential these new technologies hold for the future, as well as the role of online Open Source Communities as drivers. Chapter III discusses the associated challenges that will need to be confronted by the government, military, law enforcement, and intelligence communities both at national and international levels. Chapter IV will provide perspective via a comparative case-study review of successful and unsuccessful efforts to address these technologies as well as an overview of the online culture that is a critical piece in designing a suitable spectrum of options. Finally, Chapter V will make recommendations to address the changing strategic environment. This will include baseline options that can be used by policymakers and regulatory entities as a starting point to address current security concerns. These options are intended to be flexible enough to grow with and address future iterations of technological evolution.

[12] Siryoti, "Iran Admits Hezbollah's Drone"; Dreazen, "Next Arab-Israeli War," 1–5; Goodman and Khanna, "Power of Moore's Law," 64–73; Hanno Charisius, Richard Friebe, and Sascha Karberg, "Becoming Biohackers: The Long Arm of the Law," *BBC*, January 24, 2013, http://www.bbc.com/future/story/20130124-biohacking-fear-and-the-fbi; Devan R. Desai and Gerard N. Magliocca, "Patents, Meet Napster: 3D Printing and the Digitization of Things," *Georgetown Law Journal* 102, no. 6 (April 2014): 1691–720; Ian Paul, "'Disarming Corruptor' Disguises 3D Printing Designs to Fight the Man," *PCWorld*, November 5, 2013, http://www.pcworld.com/article/2060822/disarming-corruptor-disguises-3d-printing-designs-to-fight-the-man.html; Kyle Soska and Nicolas Christin, "Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem," paper presented at the Proceedings of the 24th USENIX Security Symposium, Washington, DC, August 12–14, 2015; Joseph C. Storch, "3-D Printing Your Way Down the Garden Path: 3-D Printers, the Copyrightization of Patents, and a Method for Manufacturers to Avoid the Entertainment Industry's Fate," *New York University Journal of Intellectual Property & Entertainment Law* 34, no. 2 (spring 2014): 249–309; Ryan Whitwam, "US State Department Begins the Nearly Impossible Task of Banning 3D-Printed Guns Online," *ExtremeTech*, July 8, 2015. http://www.extremetech.com/extreme/209461-us-state-department-begins-the-nearly-impossible-task-of-banning-3d-printed-guns-online.

THIS PAGE INTENTIONALLY LEFT BLANK

II. DEFINING THE RLT

> Remember, science fiction's always been the kind of first-level alert to think about things to come. It's easier for an audience to take warnings from sci-fi without feeling that we're preaching to them. Every science fiction movie I have ever seen, any one that's worth its weight in celluloid, warns us about things that ultimately come true.
>
> Steven Spielberg

The science fiction on screen today is in some cases only mere steps ahead of reality. Ironman's JARVIS interface is an advanced form of 3D printing coupled with cloud computing and some artificial intelligence thrown in for good measure. While Ironman is fictional, Hollywood's Legacy Effects did such a good job with the 3D printing of Ironman's movie suit that the US military has contacted them to assist with the development of the Tactical Assault Light Operator Suit, or TALOS project.[13] Many of the science-fiction storylines playing out in popular culture today are also progressing rapidly as science fact in the form of RLT.

The focus of this chapter will be on RLT, understanding what they are, how they are defined, and why these technologies are different from other disruptive technologies like the cell phone. AM provides a ready example of this family of technologies as well as ample options to demonstrate the effects that can be brought to bear by an individual technology or when multiple RLT are combined. The chapter will finish with a discussion of online Open Source Communities (OSCs) as vehicles and drivers of these game-changing technologies and the role cyberspace will play in their continued development and evolution, before moving on to Chapter III, a discussion of threat vectors.

---

[13] Peter Bright, "HP's Spout PC is Like a Real Version of Ironman's JARVIS," *ARS Technica*, October 29, 2014, http://arstechnica.com/gadgets/2014/10/hps-sprout-pc-is-like-a-real-version-of-iron-mans-jarvis/; Michael Molitch-Hou, "5 Pairs of 3D Printed Shoes You'll See at Milan Design Week 2015." *3D Printing Industry*, April 14, 2015, 1–5, http://3dprintingindustry.com/2015/04/14/5-pairs-of-3d-printed-shoes-youll-see-at-milan-design-week-2015/.

A. RLT DEFINED: CHARACTERISTICS OF THE CLASS

Defining RLT helps to bound the problem set and clarify key characteristics that must be considered when reflecting on potential spectrum solutions and formulating future policy concerning such technology.

A Radical Leveling Technology can be told from other disruptive linear technologies by the following defining characteristics:

- Anchored in the Internet whether by collaborative, developmental, or operational necessity which is core to its function and/or application
- When applied, has the effect of broad decentralization in the areas of power, economy, or information control at the nation-state level but can finely focus power and information at the individual or non-state-actor level
- Is driven in part or in whole by the strength and innovation of online OSCs
- Has a transformative and disruptive nature not just within its initial sphere of influence but across a wide range of cultural and societal processes[14]
- Has the ability, when mature, to result in a generational leap (forward or backward) that will impact global populations[15]

This class of technologies includes AM, quantum computing and cloud computing, nanotechnology, the block chain algorithm underlying the development of cryptocurrencies, advanced genetics, neurotechnology, synthetic biology, programmable materials, advanced robotics, artificial intelligence, and of course the Internet, from which all of the above derive.[16]

---

[14] James Manyika et al., "Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy," *McKinsey & Company*, May 2013, http://www.mckinsey.com/insights/business_technology/disruptive_technologies; Bill Briggs and Marcus Shingles, "Exponentials," *Deloitte University Press*, January 29, 2015, http://dupress.com/articles/tech-trends-2015-exponential-technologies/?id=us:2el:3dc:dup1012:eng:cons:tt15; John Hagel III et al., "From Exponential Technologies to Exponential Innovation: Report 2 of the 2013 Shift Index Series," *Deloitte University Press*, October 4, 2013, 1–51, http://dupress.com/articles/from-exponential-technologies-to-exponential-innovation/.

[15] Here, a generation is defined based on the generation-time equations utilized by population biologists to predict the average time between two consecutive generations. For humans, this is around twenty years. Many organizations also identify generations by title, such as the "veteran generation" or "traditionalists," 1925–45, the "baby boomers," 1945–65, and "generation X," 1965–85. Additional information and equations can be found at http://en.wikipedia.org/wiki/Generation_time or http://www.marketingteacher.com/the-six-living-generations-in-america/.

[16] Bajarin, "Most Disruptive Technology," 1–3.

RLT are different from mainstream technologies in that they pose a unique evolutionary challenge. Typically, a disruptive technology will emerge, evolve, and replace a specific pre-existing technology within a defined economic space such as the digital camera replacing film cameras or the smart phone replacing the cell phone.[17] There will also be some impact to societal processes and a few unexpected outgrowths from the disruption, but at a manageable level. RLT, however, mimic the fluidly disruptive nature of the Internet. Instead of disrupting a single specific marketplace or technology, they have the ability to disrupt and transform a wide range of processes and technologies while also significantly impacting society and culture. In a sense, RLT operate within a rapidly expanding space whose borders are constantly changing, making it difficult to anticipate and manage materializing effects.

B. ADDITIVE MANUFACTURING: THE EVOLUTION OF AN RLT

Three-dimensional printing, initially developed as "stereolithography" in 1984 by Chuck Hull of 3D Systems, was created to provide manufacturers with an affordable, rapid prototyping capability for one-off designs. The strength of AM lies in its ability to infinitely evolve digital designs and then physically manifest these items for public use. This technology, once limited to industry, became available for hobby use and hit the mainstream in 2005.[18] While AM was initially seen as a fad, the last ten years have made it apparent that this RLT is both transformative and disruptive in nature. A transformative technology is one that has the ability to change the nature or structure of how a process occurs. Experts such as Chris Anderson, Christopher Barnatt, Terry Wohlers, Peter Singer, James Canton, Toby Redshaw, and Marc Goodwin all share the opinion that AM

[17] Kyriakos Pierrakakis et al., "3D Printing and Its Regulation Dynamics: The World in Front of a Paradigm Shift," paper presented at the Proceedings of the 6th International Conference on Information Law and Ethics, Thessaloniki, Greece, May 30–31, 2014.

[18] Chuck Hull, "Pioneer in Stereolithography," *SPIE Professional*, January 15, 2013.

will have transformative effects across a broad spectrum of areas.[19] AM has also been termed a disruptive technology by these experts, and this is the more important aspect to grasp.[20] A disruptive technology will not only replace a previous technology but will evolve technology to a more advanced level or have a "groundbreaking" impact. This can be seen in technologies like the cell phone or the development of wireless communications. But unlike the cell phone, AM will not disrupt only one technology or one area; AM has the potential to disrupt multiple technologies and areas across society, replace them, and then continue to evolve. This is apparent in how the technology is advanced and employed and the impact it has on societal processes (e.g., evolving or replacing logistics structures or producing disruptive business models).[21]

There are numerous illustrations of how this RLT is causing generational leaps in various disparate fields. In 2015, AM disrupted the medical field with the first 3D-printed skull replacements, the development of 3D bioprinted capillaries and 3D-printed liver

---

[19] Chris Anderson, *Makers: The New Industrial Revolution* (New York: Crown Business, 2012); Terry Wohlers and Tim Caffrey, "Wohlers Report 2015: 3D Printing and Additive Manufacturing State of the Industry Annual Worldwide Progress Report," Wohlers Associates, 2015; Christopher Barnatt, *3D Printing: The Next Industrial Revolution* (N.p.: ExplainingTheFuture.com, 2013); Goodman, "Crime Has Gone High-Tech"; Marc Goodman, *Future Crimes: Everything Is Connected, Everyone Is Vulnerable, and What We Can Do about It* (New York: Doubleday, 2015); Goodman and Khanna, "Power of Moore's Law," 64–73; Agence France-Presse, "3D Printing Could Revolutionize War and Foreign Policy," *Space Daily*, January 5, 2015, http://www.spacedaily.com/reports/How_3D_printing_could_revolutionise_war_and_foreign_policy_999.html; James Canton, Toby Redshaw, and Rudy Burger, "New Frontiers in Emerging and Disruptive Technology: Where to Look for Innovation and Competition - and Where Not to Look," Center for Global Security Research, Lawrence Livermore National Laboratory, May 27, 2015.

[20] Wohlers and Caffrey, "Wohlers Report 2015"; Anderson, *Makers: New Industrial Revolution*; Agence France-Presse, "3D Printing Could Revolutionize War"; Barnatt, *3D Printing: Next Industrial Revolution*; Daniel Cohen, Matthew Sargeant, and Ken Somers, "3-D Printing Takes Shape," *McKinsey & Company*, January 2014; Louis Columbus, "2015 Roundup of 3D Printing Market Forecasts and Estimates," *Forbes*, March 31, 2015, 1–12; Helena Dodziuk, "What's New in 3D Printing?" *ChemViews*, February 12, 2014, doi: 10.1002/chemv.201300064; Pierrakakis et al., "3D Printing and its Regulation Dynamics"; Brian Proffitt, "How Open Source Hardware Is Driving the 3D-Printing Industry," *ReadWrite*, July 3, 2012, 1–3, http://readwrite.com/2012/07/03/how-open-source-hardware-is-driving-the-3d-printing-industry; John Pugh, "Vaccines Built on A 3D Printer," *PSFK*, November 11, 2012, http://www.psfk.com/2012/11/build-vaccines-3d-printer.html.

[21] Terry C. Pierce, *Warfighting and Disruptive Technologies: Disguising Innovation* (Abingdon, UK: Frank Cass, 2004); Anderson, *Makers: New Industrial Revolution*; Pete Basiliere, "3D Printing Predictions for 2013," *www.3ders.org*, December 30, 2012, http://www.3ders.org/articles/20121229-3d-printing-predictions-for-2013.html; Clayton Christensen, "Disruptive Innovation," Clayton Christensen website, accessed December 8, 2014, http://www.claytonchristensen.com/key-concepts/; Manyika et al., "Disruptive Technologies"; Amit Chowdhry, "What Can 3D Printing do? Here Are Six Creative Examples," *Forbes*, October 8, 2013, http://www.forbes.com/sites/amitchowdhry/2013/10/08/what-can-3d-printing-do-here-are-6-creative-examples/.

tissue, and the development of 3D-printed skin transplants using cells cultured from patients.[22] Local Motors 3D printed a new vehicle, the Rally Fighter, that consumers can customize and build themselves. Several other examples of 3D-printed autos, from Forecast 3D to the Oak Ridge National Lab and in countries like China, are now hitting the market.[23] Printed drones, airplane parts, houses, fashion, biological-based robots, and weapons are just part of the torrent impacting the marketplace and society. The convergence of AM, existing technologies, and unrestricted creativity has resulted in a revolution that will have far-reaching effects and will create sweeping cultural changes.[24] The below graphic from the Computer Sciences Corporation (CSC) report entitled *3D Printing and the Future of Manufacturing* details just a few of the areas that are being revolutionized by AM.[25]

---

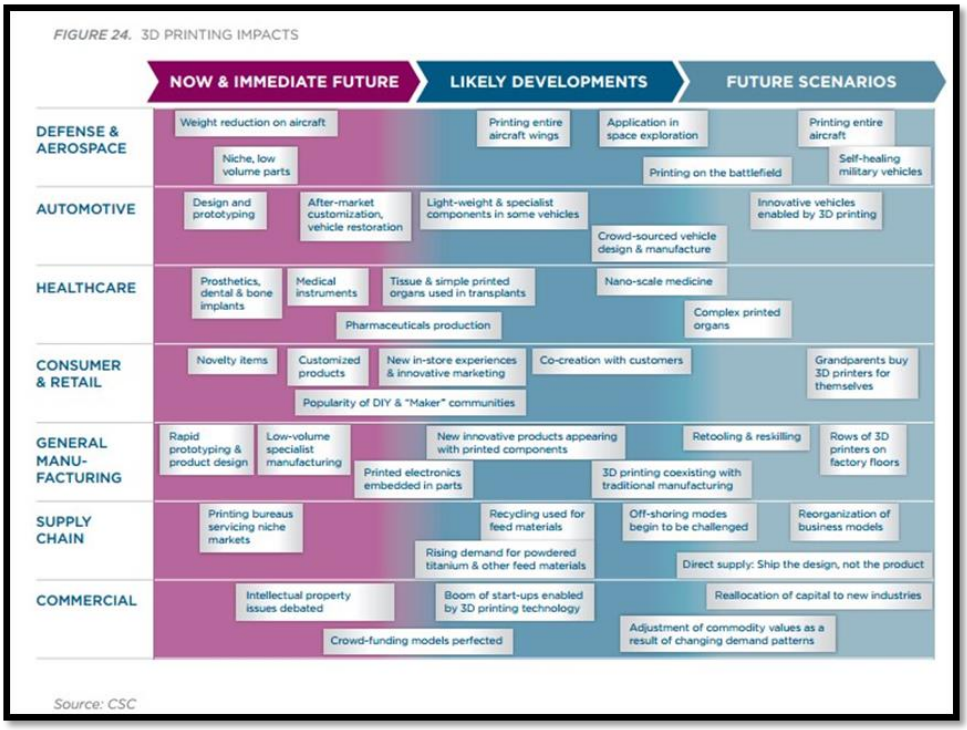
[22] "Summarized: The 3D-printing Medical Achievements of the Past Year," *Mistbreaker News*, January 3, 2015, http://www.mistbreaker.com/medicine-biotech/summarized-3d-printing-medical-achievements-past-year/.

[23] "Local Motors Rally Fighter," Local Motors, accessed May 5, 2015, https://shop.localmotors.com/products/local-motors-rally-fighter; Whitney Hipolite, "Chinese Company 3D Prints a Full-Size Working Car for Just $1770," 3DPrint.com, March 25, 2015, http://3dprint.com/53532/chinese-3d-printed-car/; Eddie Krassenstein, "Forecast 3D to Show off This Racecar, Featuring 45 3D Printed Parts at RAPID Event Next Week," 3DPrint.com, May 13, 2015, http://3dprint.com/65093/forcast-3d-printed-racecar/; David Szondy, "ORNL Unveils 3D-Printed Shelby Cobra in Detroit," *Gizmag*, January 13, 2015, http://www.gizmag.com/3d-printed-shelby-cobra-ornl/35575/.

[24] Liz Ahlberg, "Muscle-Powered Bio-Bots Walk on Command," *University of Illinois News Bureau*, June 13, 2014, https://news.illinois.edu/news/14/0630biobots2_rashidbashir.html; Adam Clarke Estes, "3D-Printed Guns Are Only Getting Better and Scarier," *Gizmodo*, January 6, 2015, http://gizmodo.com/3d-printed-guns-are-only-getting-better-and-scarier-1677747439; Materialise, "3D Print Design Show NYC," Meckler Media, accessed 5/5, 2015, http://www.3dprintdesignshow.com/; Rory Stott, "A Giant 3D Printer Builds Ten Houses in One Day," *Huffington Post*, September 2, 2014, http://www.huffingtonpost.com/2014/09/08/3d-printed-houses_n_5773408.html; Cody Wilson, "Ghost Gunner," Defense Distributed, accessed May 5, 2015, https://ghostgunner.net/; Steve Doll, "Hovership: 3D Printed Racing Drone," *Make:* 44 (April-May 2015); Michael Molitch-Hou, "US Military Turns to Hollywood's Legacy Effects to 3D Print Iron Man Suit," *3D Printing Industry*, July 9, 2014, http://3dprintingindustry.com/2014/07/09/us-military-turns-hollywoods-legacy-effects-3d-print-iron-man-suit/; David Szondy, "GE Fires Up Fully 3D-Printed Jet Engine," *Gizmag*, May 13, 2015, http://www.gizmag.com/ge-fires-up-all-3d-printed-jet-einge/37448/; Worstall, Tim. "Both GE and Rolls Royce are to use 3D Printing to make Jet Engines and Violate Engineering's Prime Commandment." Forbes (2 December 2013, 2013): 1-2.

[25] Computer Sciences Corporation Leading Edge Forum, *3D Printing and the Future of Manufacturing* (Falls Church, VA: Computer Sciences Corporation, 2012), http://assets1.csc.com/innovation/downloads/LEF_20123DPrinting.pdf.

Figure 2. 3D Printing Impacts



http://assets1.csc.com/innovation/downloads/LEF_20123DPrinting.pdf.

The advancement of RLT has in many aspects been underappreciated by policymakers and regulators; much of what has been accomplished has not been at the forefront of discussion, even of industry discussions, until recently. This is because 1) RLT display an initial value perceived to be useful in a specific and limited manner; 2) the potential for innovation by an RLT is often misunderstood or obscured by institutional bias, which leads to an incorrect assessment of the capability (typical for disruptive technologies); and 3) the development and drive behind RLT is occurring via Open Source Communities. This is and will remain the biggest challenge. These innovations are occurring in a space that many governments and policymakers still are not fully comfortable with: cyberspace. And they are being driven by the power of OSCs, which are flexible, agile, transnational, and often anonymous. These groups come

together online to apply shared expertise to AM projects, resulting in rapid prototyping and fabrication of myriad new products and processes.[26]

C. OPEN-SOURCE COMMUNITIES: DRIVERS OF EXPONENTIAL CHANGE

In order to understand the role of cyberspace and OSCs in the development of RLT, it is necessary to understand the origins of OSCs. These groups began twenty-three years ago at Helsinki University with a student by the name of Linus Torvalds. At that time, the Internet was just beginning to grow. Unix, one of the operating systems of the time, was trying to survive as a software product. A series of battles ensued; Unix split into a number of proprietary software versions all fighting against each other to become the commercialized choice, and all of them were blindsided when a company called Microsoft introduced its new operating system, Windows. For the public, many of whom were just joining the Internet, the introduction of Windows made the process of connecting much easier. Those involved with Unix feared its utility had passed. Instead, Torvalds decided to develop his own free version of Unix called Linux. Linux is one of the major ripples that helped to create the tsunamis behind the power of OSCs today. When Torvalds released Linux online, he established the first open-source online community.[27]

Most software developed at this time was created by a single programmer and released to the public to provide inputs or identify bugs so the company could fix them. In his splendid work on the history of open source entitled *The Cathedral and the Bazaar*, hacker[28] Eric Raymond uses a classic analogy for what happened next. The typical approach to software development was top down, a centralized hierarchical process that

---

[26] Joseph L. Bower and Clayton M. Christensen, "Disruptive Technologies: Catching the Wave," *Harvard Business Review* 73, no. 1 (January-February 1995): 43–53.

[27] Eric Raymond, *The Cathedral & the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*, 3rd ed. (Sebastopol, CA: O'Reilly, 2001).

[28] The term *hacker* as used here is a positive term and refers to an online member who participates in the creation of tools and software in an effort to positively influence both scientific and social processes. In the case-studies section, the term *hacker gang* is used to refer to negative actors who choose to defy the cultural norms of online OSCs and conduct illicit activities against public, private, corporate, or government entities.

Raymond categorizes as the building of a cathedral. This was done by an individual or small team and kept in house by the company until the software was ready for release. Torvalds turned this process on its head. Instead of choosing to follow the cathedral approach, he released his new code online and invited the masses to get involved in its development. As more and more people began to participate in the project, Torvalds continued to solicit input, provide updates, and delegate responsibility for specific portions of the project to smaller groups or individuals working on their own in a decentralized manner. These groups would then add their work back into the code whenever they wanted. To Raymond, the developing Linux community looked like a diverse, bustling bazaar. Brooks's law, a constant in the commercial-software-development community, implies that this type of approach should not work because communications are a significant factor. The law states, "Adding more programmers to a late project makes it later." This is because the work isn't easily shared, due to its technical nature. New programmers take time to train, causing a lapse in productivity as the experienced programmers turn their attention away from the product to help bring their peers up to speed. In theory, Torvalds's approach should have failed. Instead, Linux became one of the most successful operating systems in existence.[29]

Raymond postulates in his book that this may be due to something sociologists refer to as the Delphi effect or the Delphi method. The terms refer to the employment of structured communications in such a way as to allow a group of individuals to work collaboratively at the same time on problems of varying complexity.[30] In 2002, Murray Turoff and Harold Linstone produced a 618-page tome on the Delphi method examining its use across various group-problem-solving situations. Unsurprisingly, Delphi seemed to be a natural fit for organizations operating in cyberspace. Turoff and Linstone call this "real-time Delphi," where costs of operations are limited to the price of a computer and the use of the infrastructure that communications flow across.[31] The defining

[29] Raymond, *Cathedral & the Bazaar*.

[30] Ibid.

[31] Harold A. Linstone, and Murray Turoff, eds., *The Delphi Method: Techniques and Applications*. (Information Systems Department, New Jersey Institute of Technology, 2002), http://is.njit.edu/pubs/delphibook

characteristics of real-time Delphi include equal flow of information to and from all members at all times, improved efficiency, and the ability to limit psychological effects (observables like social class, ethnicity, language, or schooling which in some cases may interfere with individual participation in groups) due to anonymity and the establishment of open forums to air disagreements or argue critical points. This process is characteristic of OSCs operating today. The public is probably most familiar with this process in the form of "crowdsourcing," seen on startup websites like Kickstarter, or from social media events.[32]

OSCs have at their core a very effective decentralized structure. This structure allows for simultaneous sharing of information by hundreds to thousands of contributors while also providing the opportunity for feedback. Individuals also have the power to significantly influence the direction of the OSC through forums. Individual inputs are offered a certain degree of anonymity within the group, which increases participation. Individuals volunteer to work on specific portions of a problem and are selected based on their skills as well as their desires. The leader of any OSC is the person who first presents the problem to the masses and requests their assistance; however, the term *leader* must be viewed very loosely when discussing OSCs. A leader in this environment is really just a coordinator, someone who gives the group a goal and then enables the work. In some cases, this may also be a loose core group. It is interesting to note that these individuals are not necessary to the OSC's success. Individuals in a leadership function could be offline for a day or a year. It does not matter; the rest of the community will remain mobilized and continue to press forward on a solution. This is how the Internet expanded and continues to grow today. This is also why OSCs are able to rapidly mass and operate at net speed to solve problems in cyber- and physical spaces with very little command or control.[33]

OSCs began to expand following the opening of the Internet to the public in 1994. People formed online communities to conduct research, create models, perform planning functions, and develop transnational relationships in near-real or real time. For the first

[32] Linstone and Turoff, The Delphi Method: Techniques and Applications.

[33] Raymond, *Cathedral & the Bazaar*.

time in history, a group of two to ten thousand could assemble virtually, share information, discuss and debate, and then take that information in any direction that was useful to their goal. All of these interactions occur regularly without a centralized command and control structure, and the results are inarguably amazing. Hackers are developing open-source software at lightening speeds. Activists are able to quickly mobilize populations. And makers are able to take physical products, render them digitally, and then replicate and evolve them without limit.[34]

AM has a variety of capabilities, but the most influential are digital design and the 3D printer. Originally created to print physical items using the additive layering of plastics, 3D printers today can print in polymers, carbon fiber, and multiple types of metals and alloys, as well as graphene, chocolate, wood-based filaments, cements, and even living cells and tissue. This means that a machine can extrude (or sinter, for metal-based projects) materials onto a build table to produce an item in one solid piece without the need for subtractive methods like milling or machining. General Electric and Rolls Royce are using 3D printers to produce complex items like aircraft engines, which contain eighty-seven nozzles that can now be printed as a single structure. These printers allow complex items to be designed and produced as one piece without worry of welds failing or parts dropping off. This also makes the designs lighter, saves on materials, and improves efficiency by allowing for automated production around the clock by networked 3D printers.[35]

The iconic example of AM technology fusion can be found at the Tesla Factory in Fremont, CA. Unlike typical automotive manufacturing facilities this state-of-the-art facility is able to custom build a series of cars across a twenty-four-hour period without having to change out the line. This is done by combining advanced robotics with 3D

[34] A maker is an individual involved in the 3D-printing revolution, which allows participants to modify existing technologies and evolve them to their own specific requirements, then print them using plastic, polymers, or metal. Anderson, *Makers: New Industrial Revolution*; Barnatt, *3D Printing: Next Industrial Revolution*; Basiliere, "3D Printing Predictions for 2013"; Micah L. Sifry, "The Rise of Open-Source Politics," *Nation*, November 4, 2004, http://www.thenation.com/article/rise-open-source-politics/; Thorpe, "Internet Tax Cancelled."

[35] Szondy, David. "GE Fires up Fully 3D-Printed Jet Engine." Gizmag (13 MAY 2015, 2015): 5/5/2015-4. Worstall, Tim. "Both GE and Rolls Royce are to use 3D Printing to make Jet Engines and Violate Engineering's Prime Commandment." *Forbes* (2 December 2013, 2013): 1-2.

printers and programming them to meet variable manufacturing requirements. The plant can also be reprogrammed in minutes to produce anything from computers to parts for the International Space Station. AM has few limitations that an imaginative mind with the right materials cannot overcome.[36]

Once an item is captured digitally, it can be shared and evolved infinitely. Much of the software is open source, and it is not necessary to own a personal 3D printer (although one can build a basic printer for as little as $600 or an updated printer for $1,100, courtesy of YouTube).[37] If a design is ready to print, maker software allows users to link to an online production site, select production options, pay for the work, and wait for it to ship to their location. The ability to produce specialty items (including items that couldn't be produced before AM existed), small runs, and rapid prototypes are all strengths for this movement.[38]

In 2011, 3D printers gained in popularity as the public was exposed to Maker Faires, hackerspaces, and fab labs where technology was openly demonstrated and hands-on participation was welcomed.[39] By 2013, the first 3D-printed plastic gun had resulted in widespread media attention and a significant upswing in the numbers of both hobbyist and professional 3D-printer systems purchased worldwide.[40] In 2014, China printed ten houses in one day using cement and recycled construction materials, the Local Motors Strati car was printed in just forty-four hours in the U.S., and Solid Concepts started

[36] Freedonia Group, "Industry Study Report by the Freedonia Group: Global Demand for 3D Printing to Rise Over 20% Annually through 2017," 3D Printer Technology Forum, 2014; Anderson, *Makers: New Industrial Revolution*.

[37] Go here on YouTube to view videos of the home-built printer: Printer #1 Basic https://www.youtube.com/watch?v=46eq9fxaEds; Printer #2 Updated https://www.youtube.com/watch?v=u5azTt2nSZc.

[38] Anderson, *Makers: New Industrial Revolution*; Barnatt, *3D Printing: Next Industrial Revolution*; Basiliere, "3D Printing Predictions for 2013."

[39] Hackerspaces and fab labs are just two of the many public open manufacturing forums appearing across cities worldwide to teach people how to do AM and use the various associated tools and software.

[40] Simon Muphy and Russell Myers, "How *Mail on Sunday* 'Printed' First Plastic Gun in UK Using a 3D Printer and Then Took It on Board Eurostar without Being Stopped in Security Scandal," *Daily Mail*, May 11, 2013.

selling 3D-printed metal guns online.[41] These stories have caught the attention of the media, but there is a much deeper phenomenon occurring here: the maker movement (and the OSCs central to it) are the engine of AM, making it extremely agile, aggressively adaptable, and unlimited in scalability.[42]

One way to quantify the impact that OSCs are having on AM is to take a look at recent market predictions. Wohlers Associates, Inc., an independent consulting firm who has studied the 3D-printing industry for the last thirty years, has estimated that the industry will grow from $3 billion in revenue in 2013 to exceed $21 billion by 2020. Gartner projects global market growth to increase from $1.6 billion in 2015 to $13 billion by 2018. Siemens estimates that 3D printing will become 50% more affordable and the printing process will become up to 400% faster within five years.[43] Accessibility, ease of use, and increased affordability will continue to escalate the adoption of AM by the public and industry.[44]

For policymakers, RLT pose many challenges that require a thoughtful approach and that existing regulations and frameworks lack the flexibility to successfully address. Solutions will have to keep pace with RLT and hold up in a rapidly changing environment while still being enforceable. Such solutions cannot be conceived in a vacuum. Participation and expertise from OSCs and technology centers like Silicon Valley are an essential part of any policy or regulatory strategy dealing with RLT. Collaboration with these groups will enable government to respond to RLT effects not

---

[41] Melissa Goldin, "Chinese Company Builds Houses Quickly with 3D Printing," *Mashable*, April 29, 2014, http://mashable.com/2014/04/28/3d-printing-houses-china/; John Biggs, "Solid Concepts Announces Another 3D-Printed Metal Gun," *TechCrunch*, October 27, 2014, http://techcrunch.com/2014/10/27/solid-concepts-announces-another-3d-printed-metal-gun/; Lance Ulanoff, "World's First 3D Printed Car Took Years to Design, but Only 44 Hours to Print," *Mashable*, September 16, 2014, http://mashable.com/2014/09/16/first-3d-printed-car/; Boyle, Rebecca. "How the First Crowdsourced Military Vehicle Can Remake the Future of Defense Manufacturing." Popular Science, June 30, 2011. http://www.popsci.com/cars/article/2011-06/how-first-crowdsourced-military-car-can-remake-future-defense-manufacturing.

[42] Germain, "Next on the Open Source Horizon," 7; Proffitt, "Open Source Hardware Is Driving."

[43] Columbus, "2015 Roundup of 3D Printing Market," 1–12; Brent Balinski, "The 3D Printing Boom Continues," *Manufacturers' Monthly*, May 15, 2015, http://www.manmonthly.com.au/Features/The-3D-printing-boom-continues.

[44] Columbus, "2015 Roundup of 3D Printing Market," 1–12; Rob Williams, "Home Depot Sets up MakerBot 3D Printer Kiosks in 12 Stores," *HotHardware*, July 14, 2014; Krystina Gustafson, "Lowe's Brings 3-D Printing to Home Improvement," April 29, 2015, http://www.cnbc.com/id/102627784.

addressed by current laws and to design new laws replacing ineffective policy. Understanding RLT, OSCs, and developing threat vectors will remain fundamental to the construction of a useful strategy for endgame success.[45]

[45] McNulty, Arnas, and Campbell, "Toward the Printed World"; Zachary Davis, Michael Nacht, and Ronald Lehman, eds., *Strategic Latency and World Power: How Technology Is Changing Our Concepts of Security* (Livermore, CA: Center for Global Security Research, Lawrence Livermore National Laboratory, 2014); John Mark Mattox, "Additive Manufacturing and Its Implications for Military Ethics," *Journal of Military Ethics* 12, no. 3 (2013): 225–34, doi: 10.1080/15027570.2013.847534; Muphy and Myers, "*Mail on Sunday* 'Printed'"; Committee on Science, Security, and Prosperity, *Beyond "Fortress America": National Security Controls on Science and Technology in a Globalized World* (Washington, DC: National Academies, 2009); Pierrakakis et al., "3D Printing and Its Regulation Dynamics"; Shirky, "Internet Will (One Day) Transform Government."

THIS PAGE INTENTIONALLY LEFT BLANK

III. CHALLENGES POSED BY RLT

> In the case of nuclear physics there was an iconic experience, the mushroom cloud, that made it clear to nuclear physicists that their work had security implications. There has been no comparable iconic experience for life scientists.
>
> Dr. Jonathan B. Tucker, Monterey Institute of International Studies, speaking on synthetic biology, dual-use life science research, and biosecurity, May 12, 2010

The above quote is illustrative of many of the emerging technologies seen today. While it is impossible to predict all of the ways in which such technologies may be applied, it is possible via good multisource analysis to assess likely threat vectors. Policymakers, corporate leaders, governments, and the public will all need to have a realistic understanding of these technologies to successfully weigh potential risks while maximizing beneficial aspects. Reactive solutions will only exacerbate problem areas, so it is incredibly important to find thoughtful, realistic, educated solutions. In some cases, such as quantum computing, artificial intelligence, and nanotechnology, there are still a few years to proactively prepare to meet these challenges. Yet the challenges of technologies like AM and synthetic biology are already present and must be addressed now.[46]

This chapter will examine enabling factors that can lead to the development of RLT threat vectors. Asia, as a critical center for AM advancement, is used to highlight RLT-related counterproliferation challenges. The following examples demonstrate how the effects of RLT, technology convergence, down-skilling, accessibility, and new models of production and manufacturing are increasing the complexity of the counterproliferation space. The chapter concludes with a look at the need for proactive solutions and the importance of online-community and private-sector partners in getting the next generation of security solutions right.

---

[46] Cohen, Sargeant, and Somers, "3-D Printing Takes Shape"; John Drzik, "Error on Terror: Controlling Emerging Technology," *CNBC*, January 15, 2015, http://www.cnbc.com/id/102340274; Manyika et al., "Disruptive Technologies."

A. ENABLING FACTORS

The first step in understanding the risk, aside from establishing actor intent, is to identify enabling factors and the potential threat vectors that may follow. For RLT, one of the more important enabling factors is down-skilling, the process of reducing the level of technical expertise or complexity of use required for successful employment, thereby improving the accessibility of a particular technology and increasing the likelihood of digital diffusion and mass use. Other enabling factors that aid in the development of threat vectors are ineffective or unenforceable regulations, low or no infrastructure requirements, and anonymizing tools. These factors serve to increase risk by reducing intelligence signatures, decreasing operational footprints, and masking malicious actors and actions, which can result in the establishment of cyber safe havens.[47]

RLT will require an agility and autonomy that do not come naturally to any nation-state government. This necessitates a dedicated effort to retool military, diplomatic, intelligence, law enforcement, and associated policy and regulatory apparatuses to provide a balanced capacity that can excel equally in traditional conventional environments and asymmetric or hybrid threat situations. This issue was highlighted at a panel discussion by the Expert Advisory Group on Strategic Latency. Dr. James Canton, CEO and chairman of the Institute for Global Futures, illustrated how failure to adopt a balanced approach can turn an effective tactic into a losing methodology. He used the example of the America's system of weapons, which is focused on two things: decapitation and kinetic effects. In this, the US is exceedingly effective, but where these tactics fail time and again is in asymmetric environments. Here, the key to success is weapons systems designed to match that irregular state, to achieve influence and gain the support of the target: the population. Dr. Canton's point was that just because a tactic, technique, or procedure is effective in one set of circumstances does not mean that that same approach will be successful in another. The

[47] Storch, "Down the Garden Path," 1–59; Whitwam, "US State Department Begins the Nearly Impossible Task"; Goodman, "Crime Has Gone High-Tech," 1–2; Goodman, *Future Crimes*; Goodman and Khanna, "Power of Moore's Law," 64–73.

tools must be specific to the requirement.[48] As panel member Toby Redshaw, CEO of Kevington Advisors, noted, Kodak and Motorola refused to deviate from their winning tactics despite the fact that the digital camera and the smartphone presented a complete departure from existing technology and business models. Both of these corporate giants failed to adapt, and while not extinct, each company is a shadow of what it once was.[49] Apple and Steve Jobs, on the other hand, recognized changing circumstances and chose new tactics, removing internal roadblocks to change, eliminating institutional bias, and promoting adaptive innovation. This approach allowed Apple to make a comeback in both traditional and unconventional spaces. Apple was not afraid to step up and acknowledge that its tried-and-true tactics did not apply in this environment and a new approach was necessary.[50]

Forecasting is another challenge. Forecasting in intelligence often leads to unfulfilled expectations which are viewed as "intelligence failures."[51] In the case of RLT, the US needs to rapidly move away from longstanding practices and adapt to new structures that are successful in dealing with RLT and the decentralized, autonomous, flat, flexible organizations from which it derives. The US penchant for "keeping what works" will enable threat vectors, not prevent them.[52]

---

[48] Canton, Redshaw, and Burger, "New Frontiers"; James Canton, *Future Smart: Managing the Game-Changing Trends that Will Transform Your World* (Boston: Da Capo, 2015).

[49] Canton, Redshaw, and Burger, "New Frontiers"; Toby Redshaw, "The Big Bifurcation Battle – CIO Winners and Losers in 2015 and how to Land on the Winning Side," *Sand Hill*, January 27, 2015, http://sandhill.com/article/the-big-bifurcation-battle-cio-winners-and-losers-in-2015-and-how-to-land-on-the-winning-side/; Toby Redshaw, "The Internet of Things Isn't: A Thought Leadership Briefing on Profiting in the Next-Gen Internet," *Sand Hill*, June 22, 2015, 1–12, http://sandhill.com/exec-briefing/the-internet-of-things-isnt-a-thought-leadership-briefing-on-profiting-in-the-next-gen-internet/.

[50] Jason Fell, "How Steve Jobs Saved Apple," *Entrepreneur*, October 27, 2011, 1–2, http://www.entrepreneur.com/article/220604; Brad Stone, "Steve Jobs: The Return, 1997–2011," *Bloomberg Businessweek*, October 6, 2011, http://www.bloomberg.com/bw/magazine/the-return-19972011-10062011.html.

[51] Amy B. Zegart, "September 11 and the Adaptation Failure of U.S. Intelligence Agencies," *International Security* 29, no.4 (spring 2005): 78–34; Amy B. Zegart, *Spying Blind: The CIA, the FBI, and the Origins of 9/11* (Princeton, NJ: Princeton Univ. Press, 2009).

[52] Canton, Redshaw, and Burger, "New Frontiers."

B. RLT THREAT VECTORS: THE SHAPE OF THINGS TO COME

In the past, traditional threat vectors presented from known adversary states or, more recently, terror groups. With RLT, threats may emerge from these sources or from ignorant actors who misuse technology, resulting in new indigenous threats on the local level. Marketplace and social disruptions may also create unanticipated threat vectors, as the production and sale of unregulated products could lead to unintended health effects or long-term ecological impacts. A worst-case scenario would be the expansion of arms racing to non-state actors and developing nations as these entities seek to leverage RLT to achieve parity with national or regional actors.[53]

These threat vectors have the ability to produce global effects. This is why the international community must come together on the RLT problem set. A collaborative approach will be necessary to maintain current power structures and provide a unified response to RLT events.

At the Expert Advisory Group on Strategic Latency looking at "new challenges for strategic warning," Dr. Canton, Rudy Burger the managing director of Woodside Capital Partners, Toby Redshaw, and Dr. James Giordano, a neurotechnologist and neuroethicist from Georgetown University, shared their perspective on competition and risk in the technology marketplace with an eye toward national security. They all echoed the same concerns: a need to restructure, to be proactive, to keep pace with innovation. Mr. Burger noted that the existing enemies of the US are following the path of venture capital and will continue to do so. His statements on non-state-actor use of drone warfare against Israel highlighted how RLT are lowering technical and economic thresholds, making previously inaccessible capabilities available to non-state actors.[54] This area is further complicated by a lack of guidance and regulation. Dr. Giordano put this into context by explaining that approximately 60% of the research and development for neurotechnology is occurring in non-Western countries. These spaces are diverse,

[53] Manyika et al., "Disruptive Technologies"; Chris Phoenix, "Administrative Options for Molecular Manufacturing," Center for Responsible Nanotechnology, accessed May 5, 2015, http://crnano.org/administration.htm; Briggs and Shingles, "Exponentials."

[54] Dreazen, "Next Arab-Israeli War"; Zegart, "Coming Revolution of Drone Warfare"; Davis, Nacht, and Lehman, *Strategic Latency and World Power*.

regulation is inconsistent, and neurotechnology is advancing rapidly, yet it is still poorly understood by policymakers and regulators. Not all of these advancements are occurring within legal spaces, making the problems of safety and security more complex. Asia is a good example of how these factors are changing the proliferation environment.[55]

C. ASIA, RLT, AND THE COUNTERPROLIFERATION PROBLEM

Asia is one of the most dynamic and rapidly growing technology regions in the world.[56] Home to some of the world's busiest sea ports and a major producer of dual-use items, much of the Asian marketplace is under-regulated.[57] The establishment of advanced infrastructure, cyber cities, high-speed Internet, and new trade zones has made the region increasingly accessible to both legitimate and illicit actors. In the next ten years, this region will experience significant growth in nuclear power and chemical and biotechnology industries. Coupled with RLT, this is a recipe for an extremely complex proliferation environment.[58]

Asia has already had its share of proliferation challenges. In 2012, Filipino authorities detained an Iranian and an Austrian national for supplying dual-use goods to Iran's nuclear program and defying multiple export-control regulations. Asia also played

[55] Canton, Redshaw, and Burger, "New Frontiers"; James Giordano, Maren Holmes, and Paul Bracken, "Constraints on Exploiting Emerging S&T for Military Purposes: Is the Sky Falling," Center for Global Security Research, Lawrence Livermore National Laboratory, May 27, 2015; James Giordano, Anvita Kulkarni, and James Farwell, "Deliver Us from Evil? The Temptation, Realties, and Neuroethico-legal Issues of Employing Assessment Neurotechnologies in Public Safety Initiatives," *Theoretical Medicine and Bioethics* 35, no. 1 (February 2014): 73–89, doi: 10.1007/s11017-014-9278-4; Zegart, "Coming Revolution of Drone Warfare," 1–4.

[56] Daniel R. Russel, "Remarks by Daniel R. Russel Assistant Secretary, Bureau of East Asian and Pacific Affairs on the Trans-Pacific Partnership for the National Bureau of Asian Research Roundtable," US Department of State, April 1, 2015; Derek Thompson, "The 10 Fastest-Growing (and Fastest-Declining) Cities in the World," *Atlantic*, January 19, 2012, 1–10.

[57] Kenneth Rapoza, "The World's 10 Busiest Ports," *Forbes*, November 11, 2014.

[58] Togzhan Kassenova, "A Regional Approach to WMD Nonproliferation in the Asia-Pacific," *Carnegie Endowment for International Peace*, August 14, 2012, 1–10; Togzhan Kassenova, "1540 in Practice: Challenges and Opportunities for Southeast Asia," Stanley Foundation, May 2011.

a significant role in the highly publicized AQ Khan proliferation network.[59] To date, the US Department of Justice *Summary of Major US Export Enforcement, Economic Espionage, Trade Secret, and Embargo-Related Criminal Cases* report has tracked multiple instances of Asian businesses facilitating the purchase and transshipment of goods and equipment to nations like Iran and North Korea for use in illicit weapons programs. Companies across Asia have conducted operations to gain access to controlled technologies in efforts to further develop nuclear, chemical, or biological programs or restricted weapons technologies like missiles, sonar, or aircraft upgrades.[60] The belief that a lack of regulations addressing dual-use proliferation and illicit trade within Asian nations is the reason behind today's proliferation challenge is only partly correct. The challenge, as illustrated in the following example, is much more complex.[61]

D. WHEN PROLIFERATION GOES DIGITAL

In April of 2015, Hannah Robert, owner of two New Jersey defense contracting businesses, pled guilty to one count of conspiracy to violate the Arms Export Control Act. This crime is significant is because of how it was done. From 2010 to 2013, Robert transmitted export-controlled military drawings for the CH-47F Chinook helicopter to

[59] David Albright et al., "Additional Taiwan-Based Element of Iranian Military Goods Procurement Network Exposed," Institute for Science and International Security, September 16, 2015, 1–2; David Albright, *Peddling Peril: How the Secret Nuclear Trade Arms America's Enemies* (New York: Free, 2013); David Albright and Corey Hinderstein, "Uncovering the Nuclear Black Market: Working toward Closing Gaps in the International Nonproliferation Regime," paper prepared for the 45th Annual Meeting of the Institute for Nuclear Materials Management (INMM), Orlando, FL, July 2, 2004, 1–8; Nick Gillard, "Dual-Use Traders: The Real WMD Threat in Southeast Asia?" *Diplomat*, January 22, 2015, 1–3; Department of Justice, "Summary of Major U.S. Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases" (January 2008 to the present: updated January 23, 2015), August 2015, http://www.justice.gov/sites/default/files/nsd/pages/attachments/2015/01/23/export-case-list-201501.pdf.

[60] David Albright and Andrea Stricker, "Preliminary Assessment of the JCPOA Procurement Channel: Regulation of Iran's Future Nuclear and Civil Imports and Considerations for the Future," Institute for Science and International Security, August 31, 2015, 1–25; Albright et al., "Additional Taiwan-Based Element"; David Albright, Andrea Stricker, and Houston Wood, *Future World of Illicit Nuclear Trade: Mitigating the Threat* (Washingon, DC: Institute for Science and International Security, July 29, 2013), 1–130.

[61] Gillard, "Dual-use Traders"; Department of Justice, "Summary of Major U.S. Export Enforcement"; Albright, *Peddling Peril*; Albright and Hinderstein, "Uncovering the Nuclear Black Market."

India.[62] The following excerpt from the Department of Justice report describes the process:

> Starting in October 2010, Robert transmitted the military drawings for these parts to India by posting the technical data to the password-protected website of a Camden County, NJ, church where she was a volunteer web administrator. This was done without the knowledge of the church staff. Robert emailed [her contact in India] R. P. the username and password to the church website so that R. P. could download the files from India. Through the course of the scheme, Robert uploaded thousands of technical drawings to the church website for R. P. to download in India. On June 25, 2012, R. P. emailed Robert from India, stating in part: "Please send me the church web site username and password." The email was in reference to both an invoice to, and a quote for, an individual known to Robert as a broker of defense hardware items for an end user in Pakistan. This individual (the "Pakistan trans-shipper") employed a UAE address for shipping purposes.[63]

Cases in which digital renderings replace physical shipments used to be rare, but this form of proliferation is now common practice. Cyberspace is a safe haven that circumvents the need for transshipment, face-to-face meetings, and forged papers. The Internet affords an added degree of anonymity, with easy transactions and access to rapid information sharing all in a dynamic, digital environment that is extremely difficult to regulate via traditional legal frameworks. RLT further complicate the issue. The ability to generate and evolve digital designs via digital scanning, 3D computer-aided design, and software that enables reverse engineering complicate the threat picture. Many of the factors that make AM a growing industry favorite, like its flexibility, small footprint, reduced material requirements, and nominal waste stream, also mean that covert weapons programs will be even harder to detect. The ability to fully automate 3D-printing processes further decreases activities and signatures used to identify malicious actors. Experts such as Dr. Bruce Goodwin, associate director at large for national security policy and research at Lawrence Livermore National Laboratory, believe that the shrinking footprint of AM will challenge existing institutions. "The downside to all of

[62] Department of Justice, "Former Owner of Defense Contracting Businesses Pleads Guilty to Illegally Exporting Military Blueprints to India without a License," April 1, 2015, http://www.justice.gov/opa/pr/former-owner-defense-contracting-businesses-pleads-guilty-illegally-exporting-military.

[63] Department of Justice, "Summary of Major U.S. Export Enforcement."

this is that it could dramatically increase [nuclear proliferation] and make it harder to detect," Goodwin said at a recent American Physical Society meeting in San Antonio, Texas.[64]

The ability to 3D print in multiple materials also increases the complexity of the problem set. It may be possible to download a build file from the Internet for nuclear parts and print them out using a metal 3D printer. Traditional production methods for such parts would take scores of welds and a full assembly line requiring several months of work. Soon it will be possible to produce controlled nuclear parts using proliferated build files.[65] No longer is the problem of export control limited to the physical world. Digital build files used to guide 3D printers in the production of an object are widely available online, as is the necessary expertise. Illicit designs can be placed online in plain sight by using anonymizing software, such as Disarming Corruptor, which disguises the design as a regular object until an access code is entered to reveal its true nature. Dark Web proliferators are yet another wrinkle that will need to be considered. The possibility of non-state actors or rogue nations taking advantage of AM to produce restricted items such as nuclear weapons components and eventually the weapons themselves is a very real threat.[66]

According to "Wohlers Report 2015," roughly 27% of all industrial AM systems worldwide are currently located in Asia.[67] The weapon of mass destruction (WMD)-related threats posed to this area are growing precipitously. The increasing demand for WMD and associated technologies, the potential for nuclear arms racing as the US continues to draw down forces globally, and the failure to effectively engage Asian countries to encourage additional measures to regulate dual-use trade are all cause for

---

[64] Michael Lucibella, "Manufacturing Revolution May Mean Trouble for National Security," *APS Physics* 24, no. 4 (April 2015): 1–5; Bruce T. Goodwin, "Additive Manufacturing and High-Performance Computing: A Disruptive Latent Technology," presentation at the meeting of the American Physical Society, San Antonio, Texas, March 5, 2015; Castro, Daniel. "Should Government Regulate Illicit Uses of 3D Printing?" Information Technology and Innovation Foundation, May 16, 2013. https://itif.org/publications/2013/05/16/should-government-regulate-illicit-uses-3d-printing.

[65] Lucibella, "Revolution May Mean Trouble."

[66] Ibid.; Liat Clark, "Disarming Corruptor Distorts 3D Printing Files for Sharing of Banned Items," *Wired UK*, November 5, 2013. http://www.wired.co.uk/news/archive/2013-11/05/disarming-corruptor.

[67] Wohlers and Caffrey, "Wohlers Report 2015."

concern.[68] To date, only Malaysia and Singapore have instituted legislation in this area. Instead of just worrying about Iran or North Korea, governments must now think about how non-state actors might take advantage of proliferation networks and RLT. Current legal and regulatory frameworks cannot address this new aspect of the problem. As such, most of these technologies have avoided the scrutiny and study required to assess their disruptive potential.[69]

E. SYNTHETIC BIOLOGY AND BIOHACKING: ENABLING EXPONENTIAL PROMISE, REGULATING EXPONENTIAL THREATS

In 2013, a new technique for editing genes inside intact chromosomes was developed. Called clustered regularly interspaced short palindromic repeats–associated protein-nine nuclease, or CRISPR/Cas9, this method used bacteria to destroy viruses by using RNA that matched the viral DNA sequence to cut out specific components, making the virus ineffective. In March 2015, a paper was released on how this process could retarget any gene via RNA modification. The problem? This method can set off a chain reaction that takes modified DNA and spreads it generation by generation throughout the entire species. The process is 97% effective at converting the next generation of genes and would continue until every generation had been modified.[70]

Researchers were very concerned over the potential danger that this work could cause. As noted in their report:

> We are also keenly aware of the substantial risks associated with this highly invasive method, since the failure to take stringent precautions could lead to the unintentional release of [modified] organisms into the environment.[71]

---

[68] Gillard, "Dual-use Traders"; Gaurav Kampani, "WMD Diffusion in Asia: Heading Toward Disaster?" in *Strategic Asia 2004–05: Confronting Terrorism in the Pursuit of Power*, ed. Ashley J. Tellis and Michael Willis (Seattle: National Bureau of Asian Research, 2004), 379–425; Kassenova, "A Regional Approach."

[69] Drzik, "Error on Terror"; Gillard, "Dual-use Traders"; Kassenova, "A Regional Approach"; Nuclear Threat Initiative, "Asia Could See Growing WMD Threat, Expert Warns," August 21, 2008, http://www.nti.org/gsn/article/asia-could-see-growing-wmd-threat-expert-warns/.

[70] John Timmer, "New DNA Construct Can Set Off a 'Mutagenic Chain Reaction,'" *ARS Technica* March 23, 2015, 1–5.

[71] Ibid.

Researchers ensured that the fruit flies used in the experiment were kept behind three layers of containment, all flies no longer necessary to the experiment were immediately killed, and all manipulations were performed on anesthetized flies in a Biosafety Level 2 facility. Harvard professor and synthetic biologist Dr. George Church, however, believes additional precautions need to be considered. Church has serious concerns about publishing this type of work due to the complications that could result from a modified organism being released inadvertently or purposefully into the wild. Synthetic biology in a properly controlled lab could reap great benefits for everyone; synthetic biology outside of a safe, regulated lab could be downright dangerous. There currently are no formal guidelines governing the above process or human genome modifications. This is the problem confronting law enforcement and policymakers tasked with ensuring safe, ethical science in the era of DIY biology and biohacking.[72]

In 2012, artist Heather Dewey-Hagborg began attending a local Genspace, a public space where anyone can learn about biohacking, the art of reading and modifying DNA. Dewey-Hagborg wanted to find out how much she could learn from publically available DNA samples, so, using old gum and cigarette butts collected from her neighborhood, she isolated pieces of DNA that code for human facial features. Using a computer program, she reconstructed individual faces based on the DNA she had collected and 3D printed them for her *Stranger Visions* art display.[73] Disturbed at how easy it would be for someone to violate individual genetic privacy, Dewey-Hagborg then created Invisible, a two-part spray system sold by BioGenFutures for $99 used to destroy trace DNA. The first spray, called Erase, uses a laboratory-grade sanitizer to remove 99.5% of the trace DNA left by an individual, while the second spray, Replace, combines

[72] Timmer, "New DNA Construct"; Erin Brodwin, "New Generation of Bio-Hackers Make DNA Misbehave," *Newsweek*, June 26, 2014; David Baltimore et al., "A Prudent Path Forward for Genomic Engineering and Germline Gene Modification," *Science* 348, no. 6230 (April 2015): 36–38, doi: 10.1126/science.aab1028.

[73] Heather Dewey-Hagborg, "Stranger Visions," accessed May 7, 2015, http://deweyhagborg.com/strangervisions/about.html; Daniel Grushkin, "Artist Turns DNA from Chewed Gum into Sculptures," *Popular Science*, January 1, 2015; Sydney Brownstone, "DNA Sanitizer Will Wipe Your Identity off Everything You Touch," *Fast Company* May 9, 2014, http://www.fastcoexist.com/3030150/dna-sanitizer-will-wipe-your-identity-off-everything-you-touch, 3; Heather Dewey-Hagborg et al., "DIY Guides to DNA Spoofing," biononymous.me, accessed October 7, 2015, http://biononymous.me/diy-guides/; Victoria Woollaston, "Privacy Spray Promises to Remove All Traces of DNA from Surfaces - but Could It Be Used to Commit Crimes without Getting Caught?" *Daily Mail*, May 7, 2014, 4.

with any remaining DNA and alters it by the addition of new genetic material. Forensic experts have expressed concern that widespread use of the spray could significantly complicate criminal investigations.[74]

In 2013, a San Francisco-based biohacker team used the project-fund site Kickstarter to raise money to market glow-in-the-dark plants. For a $40 donation, backers would receive their own packets of modified seeds. The plants were genetically engineered using genes from marine bacteria. The team used a computer program to create the modified DNA sequence online and then emailed the sequence to a company in China, who synthesized and shipped the final DNA to the biohacker team. A gene gun was used to insert the new DNA into the plant, causing it to glow. The total cost for this process: $8,000. The funds raised on Kickstarter: $500,000.[75] A private technology watchdog, the ETC Group, notified the US Department of Agriculture about the project before the biohacked plants could be mailed to backers. The Department responded by informing ETC that they "were not equipped to regulate" this project. In the end, Kickstarter chose to ban the project, stating that "Projects cannot offer genetically modified organisms as a reward."[76]

While the majority of these groups operate under self-imposed ethical codes and safety protocols, there are still serious regulatory and ethical questions. Collaboratively working with these groups is one way to ensure that any unsafe projects are highlighted to law enforcement and stopped before they can pose a threat to the public. But even then, additional measures will be necessary. Yuriy Fazylov is a biohacker who has been working on genetically modifying plants so that they can survive in increased radiation

---

[74] Dewey-Hagborg et al., "DIY Guides to DNA Spoofing."

[75] Ariana Eunjung Cha, "Glowing Plant Project on Kickstarter Sparks Debate about Regulation of DNA Modification," *Washington Post*, October 3, 2013, https://www.washingtonpost.com/national/health-science/glowing-plant-project-on-kickstarter-sparks-debate-about-regulation-of-dna-modification/2013/10/03/e01db276-1c78-11e3-82ef-a059e54c49d0_story.html; Andrew Pollack, "A Dream of Trees Aglow at Night," *New York Times*, May 7, 2013.

[76] Brodwin, "Bio-Hackers Make DNA Misbehave"; Jim Thomas, "Kickstopper Letter to 'Glowing Plants' Project," *ETC Group*, May 7, 2013, http://www.etcgroup.org/content/kickstopper-letter-glowing-plants-project; Duncan Geere, "Kickstarter Bans Project Creators from Giving Away Genetically-Modified Organisms," *Verge*, August 2, 2013; James McIntosh, "Night Vision Eyedrops Improve Vision up to 50 Meters in Dark," *Medical News Today*, March 30, 2015, http://discovermagazine.com/2009/sep/04-forget-goggles-chlorophyll-eye-drops-give-night-vision.

environments. He hopes that this will be a useful trait for space travel or for disaster regions recovering from nuclear accidents. While his idea is innovative and has truly beneficial applications, his approach may be less so when considering biosafety. When asked about safety, Fazylov replied, "My plan is to make it first and ask questions later." Attitudes like this are not unusual and stem from a lack of education and information on the bigger picture. Bioterrorism threats could emerge from fringe groups drawing on knowledge from OSCs like the biohacker community, but they could just as easily evolve from an individual acting out of ignorance.

F. UNDERSTANDING THE REGULATORY GAPS

At this point, the picture should be clearer concerning the challenges presented by RLT to national and international security. The gaps in regulatory code and absence of authorities extend to the international community. A strong example is the UN's *Convention on Biological Diversity*, which does address synthetic biology but has no teeth.[77] Recently, the UN established the Ad Hoc Technical Expert Group on Synthetic Biology and tasked them with responding to nine questions including defining and differentiating between living modified organisms and synthetic biological organisms, the adequacy of existing protocols for regulating synthetic biology, a comprehensive definition of what is and is not synthetic biology, and a full assessment of likely risks and benefits.[78]

This is a prime example of just how big some of the gaps are with regard to understanding and dealing with RLT. Planning at just the regional or nation-state level will not be effective against these challenges, as they will derive from cyber-based transnational entities who won't be responsive to traditional regulation designed for state-to-state interactions. The risk governance required for RLT must be balanced. Too little regulation and the risks will dominate, too much regulation and the risks will anonymize

[77] Drzik, "Error on Terror"; Brodwin, "Bio-Hackers Make DNA Misbehave"; United Nations Environment Programme (UNEP), "COP 12 Decision XII/24 New and Emerging Issues: Synthetic Biology," 12th meeting of the Conference of the Parties to the Convention on Biological Diversity, Pyeongchang, Korea, October 6–17, 2014.

[78] UNEP. "COP 12 Decision XII."

and go to ground, obscuring dangerous activities and making them more dangerous still.[79]

President Obama's "pivot to the Pacific" is timely. According to a February 2015 report by Global Industry Analysts, Inc., the synthetic biology industry is forecast to have a compound annual growth rate of 42% between 2015 and 2020 in the Asia-Pacific region.[80] Areas like Malaysia's Multimedia Super Corridor and Singapore's cyber city program will be conducive to rapid growth and innovation for RLT by providing unregulated or minimally regulated cyberspaces to work and play in. Singapore's Infocomm Development Authority (IDA) cyber manifesto, now in its third iteration, highlights some strengths in its approach, including the promotion of security measures among individuals and businesses, comprehensive education and outreach programs, collaborative partnering with industry innovators, and most importantly an emphasis on information sharing. However, the focus is strictly on defensive measures against cyber-based attacks, not the effects of RLT. To date, discussions on RLT have been few outside of the corporate world, leaving a dangerous blind spot in global security.[81]

G. CONVERGENCE: THE EFFECTS OF EXPONENTIAL TECHNOLOGY SQUARED

So far, this chapter has examined effects of individual RLT, but it is also important to understand the impact of combining two or more RLT. Convergence is central to understanding RLT effects. Three-dimensional bioprinting provides a ready example by showing what can happen when AM and synthetic biology are brought

[79] Phoenix, "Options for Molecular Manufacturing"; Regan W. Damron and William Busch, "Game Changing Developments in the Proliferation of Small Arms and Light Weapons Part 2 of 2: Additive Manufacturing," EUCOM J2: EUCOM ECJ2 Strategy Division, Deep Futures, 2013; Regan W. Damron and Brian G. Henke, "Game-changing Developments in the Proliferation of Small Arms and Light Weapons, Part 1 of 2: Anonymizing Technologies," EUCOM J2: EUCOM ECJ2 Strategy Division, Deep Futures, February 5, 2013.

[80] Global Industry Analysts, Inc., "Global Synthetic Biology Market: Trends, Drivers, and Projections," accessed May 7, 2015, http://www.strategyr.com/MarketResearch/Synthetic_Biology_Market_Trends.asp.

[81] Nandikotkur, Geetha. "Assessing Singapore's Cyber Manifesto." infoRisk Today, January 23, 2015. http://www.inforisktoday.com/assessing-singapores-cyber-manifesto-a-7829/op-1. Digital Malaysia. "What is MSC Malaysia?" Accessed May 7, 2015. http://www.mscmalaysia.my/what_is_msc_malaysia.

together. While the effects of single RLT are exponential, a merger of these technologies can create effects that are much grander in scale.[82]

Three-dimensional bioprinting is the process by which a modified 3D printer uses cells to build anything from skin or organ tissues to organs themselves. This market is moving forward at double the exponential rate thanks to the convergence of 3D bioprinting, robotics, and advanced genomics. New approaches in the field of biology have also helped enable this rapid development. For example, researchers now view biology not just as a science but also as an information technology. This new perspective has changed scientific processes into much faster information processes. Researchers can now use 3D bioprinters like the BioAssemblyBot (BAB) and its associated Tissue Structure Information Modeling (TSIM) program to scan cellular structure and organs, then import them into modeling programs for study or printing. Prior to this advancement, teams would spends weeks and months on coding and scripts just to be able to scan and model small features. What typically would take a team half a summer to do can now be accomplished in half a day.[83]

Three-dimensional-printed skin for burn victims, synthetic vaccines, cells for drug testing, and organs all exist today. This is revolutionizing medicine and changing how illness and disease will be treated in the future. Viruses like Ebola and Marburg could be eradicated using targeted vaccines that incorporate CRISPR/Cas9 to stop the pathogen from replicating. The benefits RLT convergence will be tremendous for the quality of human health worldwide.[84]

But as with all technologies, there is a dark side to consider as well. Dr. Jill Bellamy addresses one area on her website, *Biological Warfare Blog: Black Six*:

---

[82] Briggs and Shingles, "Exponentials."

[83] Gilpin, Lindsey and Jason Hiner. "New 3D Bioprinter to Reproduce Human Organs, Change the Face of Healthcare: The Inside Story." TechRepublic, August 1, 2014.

[84] Jill Bellamy, "DARPA's 7-Day Bio-Defence and the Future of Synthetic Vaccines," *Biological Warfare Blog: Black Six*, January 4, 2015, http://bio-defencewarfareanalyst.blogspot.co.uk/2015/01/darpas-7-day-bio-defence-and-future-of.html; Craig J. Venter, "First Self-replicating Synthetic Bacterial Cell," J. Craig Venter Institute, accessed May 7, 2015, http://www.jcvi.org/cms/research/projects/first-self-replicating-synthetic-bacterial-cell/overview/; Daniel G. Gibson et al., "Creation of a Bacterial Cell Controlled by a Chemically Synthesized Genome," *Science* 329, no. 5987 (July 2010): 52–56, doi: 10.1126/science.1190719.

> What if the disease we are trying to prevent is unknown, synthetically derived, and possibly created in a clandestine warfare lab? As I've previously discussed, DARPA's Blue Angel program and Medicago have successfully overcome the production lag-time issue for flu vaccine production; however, what would happen if a synthetic virus unknown at this point were able to be either accidentally or deliberately released? While I personally remain a strong proponent of synthetic biology, and political arguments aside, are we ready to treat, in a mass casualty context, synthetic illnesses?[85]

Dr. Bellamy's concerns are well founded. In 2005, a team of researchers was able to reconstruct the 1918 flu virus that was responsible for killing almost fifty million people globally, while in 2008, scientists used synthetic biology to recreate the severe acute respiratory syndrome (SARS) virus by pretending to be involved in research on combatting infectious diseases. Both of these events took place in labs with professionally trained personnel, but RLT are lowering the technical requirements, are becoming more affordable and easier to use, and are supported by a web of online experts.[86] The 2010 *Homeland Security News Wire* article "Day of Synthetic Pathogens-Based Bio-Terrorism Nears" speaks to the seriousness of the problem when considering the malicious application of such technologies:

> "The problem is that now you can make DNA. For a number of these, you really don't need to have access to the sample. The genomes of these pathogens are in publicly available databases," said Jean Peccoud, an associate professor at the Virginia Bioinformatics Institute at Virginia Tech. "For a few thousand dollars you can get the Ebola genome."[87]

---

[85] Jill Bellamy, "Treating the Unthinkable: Vaccine Development for Unknown Synthetic Viruses," *Biological Warfare Blog: Black Six*, May 19, 2014, http://bio-defencewarfareanalyst.blogspot.co.uk/2014/05/treating-unthinkable-vaccine.html.

[86] *Homeland Security News Wire*, "Day of Synthetic Pathogens-Based Bioterrorism Nears," September 16, 2010, http://www.homelandsecuritynewswire.com/day-synthetic-pathogens-based-bioterrorism-nears; Jill Bellamy, "Emerging Technologies: Lowering the Threshold for ISIS (Islamic State of Iraq and Syria) Mass Casualty Terrorism," *Biological Warfare Blog: Black Six*, July 31, 2015, http://bio-defencewarfareanalyst.blogspot.co.uk/2015/07/emerging-technologies-lowering.html.

[87] *Homeland Security News Wire*, "Synthetic Pathogens-Based Bioterrorism Nears."

Today, the Ebola genome can be freely downloaded from several websites for study or research, at school or at home.[88] Companies like Organovo, Cambrian Genomics, Parabon NanoLabs, and Johnson & Johnson are using genomic data and combining it with bioprinting to create antitoxins, vaccines, designer genetics, printed skin, and tissue, as well as new regimes of pharmaceuticals in weeks, not years.[89] Meanwhile, individuals are 3D printing viruses to fight cancer, making targeted drugs to combat disease, and manipulating biological particles in ways that are providing incredible new insights into the human machine.[90] On average, these technologies are doubling in capability every eight to twenty-four months, which means each technology will make capability advancements of a hundred to a hundred-thousand fold within the next ten years. For example, in just six years, the cost of genome sequencing went from $10 million down to a mere $1,000. In the eight months required to research and write this paper, each one of these technologies has advanced by a factor of five.[91] These revolutions will disrupt industry, processes, society, and most importantly warfare and security at an ever-increasing rate, in many cases much sooner than expected, due to the crowdsourcing power of OSCs driving these evolutions. Proactive planning and preparation of the battlespace needs to happen now, especially within special mission

[88] University of California, Santa Cruz, "Ebola Genome Portal," UCSC Genome Informatics Group, accessed May 6, 2015, https://genome.ucsc.edu/ebolaPortal/; Virus Pathogen Research, "Ebolavirus," accessed May 7, 2015, http://www.viprbrc.org/brc/home.spg?decorator=filo_ebola.

[89] Maxx Chatsko, "5 Crazy Technologies made Possible by 3-D Bioprinting," *Motley Fool*, November 12, 2013, http://www.fool.com/investing/general/2013/11/12/5-crazy-technologies-made-possible-by-3-d-bioprint.aspx; Scott Grunewald, "Cambrian Genomics 3D Printing DNA—Sets Its Sights on Space Dinosaurs," *3D Printing Industry*, April 10, 2014, http://3dprintingindustry.com/2014/04/10/cambrian-genomics-3d-printing-dna/.

[90] Bridget Butler Millsaps, "Autodesk Genetic Engineer Is Able to 3D Print Viruses, Soon to Attack Cancer Cells," *3DPrint.com*, October 17, 2014, http://3dprint.com/19594/3d-printed-virus-fights-cancer/; Pugh, "Vaccines Built on a 3D Printer"; Paul Marks, "3D Printing and Augmented Reality to Help Model Drugs," *NewScientist*, October 18, 2011, 2, http://www.newscientist.com/blogs/onepercent/2011/10/3d-printed-viruses-meet-their.html.

[91] Geoffrey Shmigelsky, "Exponential Technology," Think Exponential, accessed May 6, 2015, http://thinkexponential.com/invest/exponential-technology/; Brian Krassenstein, "The Moore's Law of 3D Printing… Yes It Does Exist, and Could Have Staggering Implications," *3DPrint.com*, June 28, 2014, http://3dprint.com/7543/3d-printing-moores-law/.

units and those units most likely to be tasked with dealing with negative aspects of these advancements.[92]

H. THE NEED FOR A NEW PARADIGM

The intent of this chapter was to illustrate the speed, complexity, challenges, and gaps in the RLT space. The majority of RLT users seek to make the world a better place, which is why understanding technology and regulatory concerns is the first step toward finding solid solutions. How the government chooses to interact with OSCs can make the difference between sound policy and good intelligence or ineffective policy and getting blindsided by an exponential 9/11. The key to next-generation security will be found within these groups and their ethical efforts. Trust, transparency, partnerships, and active collaboration are all necessary for success. As the following case studies demonstrate, there are right ways and wrong ways to approach the online community. Understanding the culture, whom to partner with, and how is paramount to international security.[93]

---

[92] Shmigelsky, "Exponential Technology"; Jennifer Hicks, "3D Printed Virus to Attack Cancer Cells," *Forbes*, October 29, 2014.

[93] David Silver, "Introducing Cyberculture," Resource Center for Cyberculture Studies, University of San Francisco, last modified December 10, 1999, http://rccs.usfca.edu/intro.asp; Toby Redshaw, "The Internet of Things Is Not the Next Big Story for the Internet," *Sand Hill*, June 24, 2015, http://sandhill.com/article/the-internet-of-things-is-not-the-next-big-story-for-the-internet/; Samir Chopra and Scott Dexter, "The Political Economy of Open Source," *International Journal of Technology, Knowledge, and Society* 1, no. 1 (2005): 1–14; Chris DiBona, Sam Ockman, and Mark Stone, eds., *Open Sources: Voices from the Open Source Revolution*, (Sebastopol, CA: O'Reilly, 1999); Jeremy Heimans, "What New Power Looks Like," TED video, 15:08, June 2014, https://www.ted.com/talks/jeremy_heimans_what_new_power_looks_like?language=en.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. NAVIGATING THE COMPLEX CULTURE DRIVING RADICAL LEVELING TECHNOLOGIES

> In the life sciences, researchers and security officials hadn't much history of working together. After 9/11, tensions threatened to grow between them. Neither group understood how the other operated and each thought the other was basically clueless.
>
> Gerald Epstein, Director AAAS Center for Science, Technology and Security Policy

In 2012, a company called Defense Distributed became the first producer of a 3D-printed firearm, called the Liberator. Intended by the group to be a political statement concerning the protection of constitutional freedoms online and to send a message to global governments about the regulation of digital technologies, the project was quickly misinterpreted as a significant threat to security. The State Department officially requested that Defense Distributed remove the designs from their website, indicating that the files may be subject to the International Traffic in Arms Regulations (ITAR), a policy responsible for regulating weapons and certain kinds of technical data. The group complied, but not before over a hundred thousand downloads of the design had been recorded.[94] Today, it is easy to find and download the original files from numerous online locations. A second statement by the State Department issued in June 2015 took a stronger stance on the issue of 3D gun design, declaring the intent to restrict specific types of designs and to require developers to obtain approval before "online publication of any technical data that . . . would allow for the creation of weapons . . ."[95]

---

[94] Danton Bryans, "Unlocked and Loaded: Government Censorship of 3D Printed Firearms and a Proposal for More Reasonable Regulation of 3D Printed Goods," *Indiana Law Journal* 90, no. 2 (April 2015): 901–34; Tara Dodrill, "Breaking: Government Claims Control of Wiki Weapons Project," *Off the Grid News*, accessed August 3, 2015, http://www.offthegridnews.com/self-defense/guns-ammo/breaking-government-claims-control-of-wiki-weapons-project/; Andy Greenberg, "Feds Tighten Restrictions on 3D Printed Gun Files Online," *Wired*, June 11, 2015, 1–11; Julian J. Johnson, "Print, Lock, and Load: 3-D Printers, Creation of Guns, and the Potential Threat to Fourth Amendment Rights," *University of Illinois Journal of Law, Technology & Policy* 2 (2013): 337; Jon Lawrence, "3D Printing: Legal and Regulatory Issues," *Electronic Frontiers Australia*, August 8, 2013, https://www.efa.org.au/2013/08/08/3d-printing-issues; Steven Levy, "Crypto Rebels," *Wired*, January 2, 1993, 1–14.

[95] Greenberg, "Feds Tighten Restrictions."

This is one example of many in which a cultural misunderstanding complicated a situation that could have been resolved in a much simpler fashion. Understanding that Defense Distributed is an outgrowth of an online cultural group known as the cypherpunks, who are dedicated to the protection of individual user rights online, especially freedom of speech and expression, may have influenced the State Department to take a different approach. The case studies in this chapter will underscore three primary themes of attempts to utilize traditional methods of regulation against this problem set: 1) a lack of understanding of cultural norms and moral issues will negate applied legal measures, 2) a failure to understand and incorporate the cultures of the regulatees will lead to failed policy, and 3) the negative effects of applying quick policy fixes to RLT and online OSCs can cause nations to be less secure and grant a foothold for rogue actors.

While the State Department's intentions were to enhance public safety, the effect achieved was the opposite. Within days of the June announcement, online groups that had been openly discussing 3D printing firearms suddenly instituted private chat rooms, deleted comments on how to meet existing gun laws or ways to circumvent the law, and began looking to encryption programs or Dark Web servers sponsored by foreign entities to escape US jurisdiction. Any visibility that open-source analysts had on this particular technological evolution, how quickly the technology was diffusing, and which groups might be willing to collaborate with the government to conduct self-policing or threat warning disappeared overnight. This phenomenon is not new, yet it continues to pose a stumbling block to regulators. As in the battle by MGM to stop illegal music sharing, the danger of making a moral issue into a market issue means that legal measures, especially measures that are likely to have little to no impact, generally result in anonymizing behaviors, high rates of diffusion via digital means, and isolation of user groups, restricting participation in constructive, collaborative solution forums. The technology evolves in exactly the manner the regulator had hoped to avoid.[96] One reporter did a good job of summing up the ill-conceived regulation strategy:

[96] Paul, "'Disarming Corruptor'"; Storch, "Down the Garden Path"; J. D. Tuccille, "After Silk Road, Online Marketplaces for Drugs and Weapons Grow, with More to Come," *reason.com*, August 25, 2015, 1–3, https://reason.com/archives/2015/08/25/after-silk-road-online-illicit-marketpla.

> Even those who do not feel that everyone should have the ability to print their own guns have to see the lopsided logic at blocking access to the 3D printable gun instructions when directions on how to craft fertilizer bombs and make poisons [are] still readily available.[97]

Technological change can be daunting. But it is important to recognize when that change is occurring and then take the time to formulate an appropriate response. Failure to do so can make a simple political statement into a much bigger problem.[98] The Liberator demonstrates the impact the lack of understanding of the "foreign" culture of OSCs and the influence (or lack thereof) that cookie-cutter policies and outdated regulations can have. While cultural training is stressed for military and diplomats operating in foreign nations, it is seldom discussed in terms of cyber and technology policy. This shortsightedness has a cost: alienated and radicalized OSCs, an online community that fails to report apparent threats to national security or public safety, stifled innovation that damages the US economy and military, and the creation of dangerous blind spots that can function as cyber safe havens for nefarious actors. The most important factor in the development of policy is understanding the culture and environment in which that policy needs to operate. This chapter will be devoted to identifying successful and failed attempts to engage with OSCs, to provide an understanding of some of the critical nuances explicit to policy and regulation in the digital dimension. Without this grounding, RLT policy development will at best have limited success or at worst be a total failure that results in enhanced operational security for threat actors.[99]

This chapter will provide an introduction to the online open-source culture. While groups may have their own unique personalities, all online groups embrace a shared cyber culture and (with the exception of a radical minority) obey its mandates. The case-study segment will follow, with five examples of negative interactions between government or corporate actors and OSCs (to include individual actors), highlighting

---

97 Dodrill, "Government Claims Control."

98 Paul, "'Disarming Corruptor'"; Storch, "Down the Garden Path"; Tuccille, "After Silk Road."

99 Levy, "Crypto Rebels"; Paul, "'Disarming Corruptor'"; Storch, "Down the Garden Path"; Tuccille, "After Silk Road."

what went wrong, why, and the end results (costs) of the interaction. A look at existing policy and identified shortfalls using 3D printing as an example will be included. Then, five positive case-study interactions will be examined with a focus on why these interactions were successful and what government and corporate entities did differently to make them a success. Finally, the chapter will conclude with a discussion of elements that can help to craft smart policy for the digital environment while avoiding known pitfalls that can lead to the "compliance without effect" problem experienced by policymakers grappling with RLT today.[100]

A number of academic and research centers have begun to study cyber culture and the culture of online communities in order to understand their norms, values, and beliefs. While some groups are very accessible, like the makers, others, like cyber gangs, can be more reclusive and harder to study.[101] A good starting point for understanding OSCs and their culture can be found in the groups that represent them and their concerns in public. The Electronic Frontier Foundation is one of the primary public-action groups within the United States representing individuals and groups in the digital world. Their focus on "free speech, fair use, supporting innovation, privacy, freedom of expression, and transparency" is a good representation of what many online OSCs are about. The majority of "netizens" seek to use their actions online and in advancing technology to

[100] Bryans, "Unlocked and Loaded."

[101] Richard Kahn and Douglas Kellner, "Internet Subcultures and Oppositional Politics," Post-subcultures Reader (2003): 299–314. https://pages.gseis.ucla.edu/faculty/kellner/essays/internetsubculturesoppositionalpolitics.pdf; Donna Gibbs and Kerri-Lee Krause, eds., *Cyberlines 2.0: Languages and Cultures of the Internet* (James Nicholas, 2006); Richard Kahn and Douglas Kellner, "New Media and Internet Activism: From the 'Battle of Seattle' to Blogging," *New Media & Society* 6, no. 1 (February 2004): 87–95, doi: 10.1177/1461444804039908; Alison Powell, "Emerging Issues in Internet Regulation: The Unstable Role of WikiLeaks and Cyber-Vigilantism," in *Research Handbook on Internet Governance*, ed. Ian Brown (Northampton, MA: Edward Elgar, 2012); Rheingold, Howard. Smart Mobs: The Next Social Revolution. Cambridge, MA: Perseus Publishing, 2003.

improve the world and have chosen to obey the core rules of "netiquette."[102] These rules include such items as "remember the human, adhere to the same standards of behavior online that you follow in real life, share expert knowledge, respect other people's privacy, and don't abuse your power."[103] They also identify "cyberspace predators, alternate or anonymous persona usage, electronic forgery, chain letters and hoaxes, email harassment, worms, viruses, snooping, and mailbombing" as "egregious violations of netiquette."[104] The culture is one of respectful freedom that values collaborators, open dialogue, and passionate discourse on the way the world is and how to improve it. Online reputation is everything. This is because the online culture is a gift culture.[105] Reputation and credibility are the currencies of success. Hacker Eric Raymond highlights why the features of the gift culture specific to the online community are so very central:

> There are reasons general to every gift culture why peer repute (prestige) is worth playing for: First and most obviously, good reputation among one's peers is a primary reward. We're wired to experience it that way for evolutionary reasons touched on earlier. . . . Secondly, prestige is a good way (and in a pure gift economy, the only way) to attract attention and cooperation from others. If one is well known for generosity, intelligence, fair dealing, leadership ability, or other good qualities, it becomes much easier to persuade other people that they will gain by association with you. Thirdly, if your gift economy is in contact with or intertwined with an

---

102 "Electronic Frontier Foundation," Electronic Frontier Foundation, accessed July 27, 2015, https://www.eff.org/issues; "RIAA v. the People: Five Years Later," Electronic Frontier Foundation, September 30, 2008, https://www.eff.org/en-gb/wp/riaa-v-people-five-years-later; Jordan S. Hatcher, "Of Otakus and Fansubs: A Critical Look at Anime Online in Light of Current Issues of Copyright Law," *SCRIPT-Ed* 2, no. 4 (December 2005): 545–71, doi: 10.2966/scrip.020405.514; Corinne Miller, "The Video Game Industry and Video Game Culture Dichotomy: Reconciling Gaming Culture Norms with the Anti-Circumvention Measures of the DMCA," *Texas Intellectual Property Law Journal* 16, no. 1 (spring 2008): 453–83; H. Brinton Milward and Jörg Raab, "Dark Networks as Organizational Problems: Elements of a Theory," *International Public Management Journal* 9, no. 3 (2006): 333–60; Howard Rheingold, "The Virtual Community," accessed August 25, 2015, http://www.rheingold.com/vc/book/; Virginia Shea, "Netiquette," Albion.com, accessed August 25, 2015, http://www.albion.com/netiquette/; Silver, "Introducing Cyberculture"; Soska and Christin, "Measuring the Longitudinal Evolution."

103 Shea, "Netiquette"; Cory Doctorow, "How Laws Restricting Tech Actually Expose Us to Greater Harm," *Wired*, December 24, 2014: 1–13, http://www.wired.com/2014/12/government-computer-security/; Eric Hughes, "A Cypherpunk's Manifesto," Activism.net, March 9, 1993, http://www.activism.net/cypherpunk/manifesto.html; Levy, "Crypto Rebels"; Silver, "Introducing Cyberculture."

104 Shea, "Netiquette."

105 H. Peyton Young, *Individual Strategy and Social Structure: An Evolutionary Theory of Institutions* (Princeton, NJ: Princeton Univ. Press, 2001); Raymond, *Cathedral & the Bazaar*; Rheingold, "Virtual Community."

> exchange economy or a command hierarchy, your reputation may spill over and earn you higher status there . . .[106]

This explains in part why OSCs frequently self-police and when individuals or groups are found to be breaking the rules of the online community it is taken seriously. Credibility both in cyber and in real life (IRL) matters. This can be seen in hundreds of actions taken daily to stop criminal acts, to create and not destroy the Internet, and to protect public safety. From the use of social media networks to catch criminals in Philadelphia to the actions of hackers to stop an online gang from ruining Christmas for Xbox gamers to the work of hacktivist groups like Anonymous to voluntarily combat the online hatred of ISIS, the online community is striving to make a positive difference. There are hundreds of thousands of cyber citizens who are born collaborators, subject-matter experts, problem solvers, and cyber-community-watch members creating an untapped resource for increasing security capacity at an international level. That is why understanding the underlying culture of OSCs, much like understanding the culture of a foreign nation, is the first step in addressing the challenges of RLT while still guaranteeing innovation and the protection of freedoms.[107]

The case studies that follow highlight examples of interactions between government officials, corporate officials, and entities involved with new technologies and processes within the cyber realm. The goal is not to identify every policy pitfall or policy win, but to show a range to establish a baseline for policymakers to work from. RLT are and will likely remain inextricably tied to the digital world, so the case studies focus on

---

106 Raymond, *Cathedral & the Bazaar*; Rheingold, "Virtual Community."

107 Kelly Bayliss, "Gay Couple Beaten in Possible Hate Crime Attack: Police," *NBC 10 Philadelphia* video, 2:26, September 12, 2014, http://www.nbcphiladelphia.com/news/local/2-Gay-Men-Attacked-by-Group-Center-City-274964621.html; "Social Media Sleuth Helps Catch Police Chief's Daughter Charged in Gay Bashing," *Inside Edition* video, September 26, 2014, http://www.insideedition.com/headlines/8996-social-media-sleuth-helps-catch-police-chiefs-daughter-charged-in-gay-bashing; James Cook, "How a Hacker Gang Literally Saved Christmas for Video Game Players Everywhere," *Business Insider*, December 16, 2014: 1–5, http://www.businessinsider.com/lizard-squad-hack-playstation-and-xbox-2014-12?r=UK&IR=T; Anthony Cuthbertson, "Anonymous Lists 9,200 Twitter Accounts Linked to Islamic State After Hactivist Collaboration," *International Business Times*, March 16, 2015, 1–4, http://www.ibtimes.co.uk/anonymous-lists-9200-twitter-accounts-linked-islamic-state-after-hacktivist-collaboration-1492035; RFSID, "Lizard Squad: Two Bot Thugs," *Recorded Future*, January 19, 2015, https://www.recordedfuture.com/lizard-squad-analysis/; Vandita, "Anonymous Takes down ISIS Websites, Confirms Leaked Government Documents Were Real," Anonymous HQ, accessed January 29, 2015, http://anonhq.com/anonymous-takes-isis-websites-confirms-leaked-government-documents-real/.

examples that provide data points necessary for success in policy development for the digital environment. The first set of case studies, of adverse interactions, includes *MGM v. Grokster*, *Bernstein v. Department of Justice*, *Junger v. Department of State*, *LightSquared v. GPS*, and a dual case examination of *Defense Distributed v. Department of State* and the 3D-printed gun ban implemented by the city of Philadelphia. In the final case study, the two examples are intertwined and have several important aspects that pertain to regulating today's digital environment.[108]

A. *MGM V. GROKSTER*: THE PEER-TO-PEER PROBLEM

In February of 2000, MGM led a joint industry suit against peer-to-peer (P2P) music distributors and a group of individual P2P users and developers, claiming that these services were leading to a reduction in revenue. The company's intent was to protect intellectual property rights and to deter any future P2P projects from gaining traction. To the point, the courts found in favor of MGM. Yet despite the ruling and additional prosecutions, instances of P2P use continued to increase. An anthropological illustration used by Brafman and Beckstrom paints the picture of what happened next. Much like Cortés and the Spanish conquest of the Americas, MGM was successful in its efforts to target and force the startup P2P entities to stop. However, that targeting caused the OSCs at work to adapt their network structures, becoming like Cortés's nemesis: the Apache tribe. Cortés's initial success was due to the fact that he was pitted against hierarchical networks with well-defined centers of gravity. The Aztecs and Incan cities

---

108 Anonymous, "FBI Using Information from Anonymous to Help Find US Central Command Hackers," Anonymous Activism, accessed January 29, 2015, http://anonhq.com/; Ori Brafman and Rod A. Beckstom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations* (New York: Penguin, 2006); Bryans, "Unlocked and Loaded"; Jean Camp and Ken Lewis, "Code as Speech: A Discussion of Bernstein v. USDOJ, Karn v. USDOS, and Junger v Daley in Light of the U.S. Supreme Court's Shift to Federalism," *Ethics and Information Technology* 1, no. 2 (August 2001): 1–13; Cook, "Hacker Gang Literally Saved Christmas"; Cuthbertson, "Anonymous Lists 9,200 Twitter Accounts"; Desai and Magliocca, "Patents, Meet Napster"; Johnson, "Print, Lock, and Load"; Lawrence, "3D Printing: Legal and Regulatory Issues"; Edward Lempinen, "FBI, AAAS Collaborate on Ambitious Outreach to Biotech Researchers and DIY Biologists," *American Association for the Advancement of Science*, April 1, 2011, http://www.aaas.org/news/fbi-aaas-collaborate-ambitious-outreach-biotech-researchers-and-diy-biologists; Pamela Samuelson, "Three Reactions to MGM v. Grokster," *Michigan Telecommunications and Technology Law Review* 13 (2006): 177–96; Storch, "Down the Garden Path"; Joel Waldefogel, "Digitization, Copyright, and New Media Products: Evidence from Recorded Music," presentation, Global Governance Programme, December 14–15, 2012, http://globalgovernanceprogramme.eui.eu/wp-content/uploads/2013/01/Joel-Waldefogel.pdf.

were easy prey for the Spanish and their conventional tactics, but all that changed with the Apache. The Apache were nomads, with no defined leadership structure or key terrain that the Spanish could target. Cortés's strategy started to fall apart, and the Apache succeeded in driving him from their lands.[109]

Similar to the Apache, the decentralized nature of OSCs created an overmatch to the music industry's strategy. The more the music industry fought against these OSCs, the stronger they became. OSCs adopted increasingly decentralized open structures to defeat identifying measures that could lead to prosecution. P2P servers moved offshore or outside of US jurisdiction and developed serverless software, evolving into Grokster, eDonkey, and later eMule, each more impervious to MGM's attempts at regulation. EMule was an especially brilliant bit of innovation. It was the first open-source P2P software with no known author, and it functioned autonomously online. It became the bulletproof standard for combatting regulation of P2P sharing. Without any targetable information, MGM had no way to stop the sharing. EMule continues to function across the web today.[110]

The actions taken by MGM were meant to make P2P file sharing a highly visible crime but instead made the problem of copyright infringement worse. By setting a low price (cost of action) on the violation, MGM turned a moral issue, stealing, into a market issue, a risk-benefit equation in which the risk continued to decrease while legal costs remained the same. This encouraged P2P adoption by a greater segment of the population. The other problem confronting MGM was one of bias. Big organizations tend to suffer from the belief that 1) the status quo is the best option, 2) change will require a departure from the organization's current capabilities and may be more costly, so 3) the organization refuses to abandon them even if they are consistently losing ground to other methods. In deterrence theory, the concept of punishment resulting in specific costs

[109] Electronic Frontier Foundation, "RIAA v. the People: Fiver Years Later"; Brafman and Beckstom, *Starfish and the Spider*; Bryans, "Unlocked and Loaded"; Desai and Magliocca, "Patents, Meet Napster"; Samuelson, "Three Reactions"; Waldefogel, "Evidence from Recorded Music."

[110] Brafman and Beckstom, *Starfish and the Spider*; David Xanatos and Ekliptor, "EMULE: A Decade of File Sharing Innovations," TorrentFreak, May 13, 2012, https://torrentfreak.com/emule-a-decade-of-file-sharing-innovations-120513/.

should function to limit the unwanted behavior. Yet in cases like *MGM v. Grokster*, a "motivation crowding" effect occurs. This is when individual actions are incentivized toward compliance or defiance of a regulation based on external factors such as a fine or a bonus. These external factors change the moral principles that have been in play (don't steal because stealing is bad), replacing them with an action based on marketplace calculations (I can legally buy this music or I can get it for free online with very little risk of getting punished). In the case of P2P file sharing, the effects of MGM's actions can be explained as follows:

> The external monetary motivation of the industry lawsuits crowded out the internal incentive to act in an honest way and pay for the content one acquires. 'Civic virtue (a particular manifestation of intrinsic motivation) … bolstered if the public laws convey the notion that citizens are to be trusted,' was undermined by the industry's actions in pursuing lawsuits against individuals. Conversely when citizens feel that they are not trusted, they react by breaking the law if they expect the cost of doing so to be low. In a study, students who already shared files reported that heavy sanctions led them to believe their behavior was more ethical than moderate sanctions did.[111]

MGM and its industry partners spent millions trying to stop P2P technology, and in the end their efforts had very little effect. Today, digital music is available from a number of online for-pay vendors as well as via P2P sources. Recent studies have even found that P2P has been beneficial to big music. Music quality is up, cost is down, a much bigger pool of talent is available to recruiters, and revenue has increased thanks to new digital music products.[112] The very "unpredictability and experimentation" that characterizes the digital environment served to expand the digital marketplace for music.[113]

In the case of MGM, the policy and regulation attempts failed due to bias (status quo bias and endowment effect), a misunderstanding of how application of policy via

---

[111] Storch, "Down the Garden Path."

[112] Waldefogel, "Evidence from Recorded Music."

[113] Electronic Frontier Foundation, "RIAA v. the People: Fiver Years Later"; Brafman and Beckstom, *Starfish and the Spider*; Desai and Magliocca, "Patents, Meet Napster"; Samuelson, "Three Reactions"; Waldefogel, "Evidence from Recorded Music."

legal means would change the equation from a moral calculation to one of price setting, and a lack of clarity about the desired end state. The result was the proliferation of a disruptive technology. This interaction resulted in lost time and resources for MGM as well as bad relations with the OCSs behind P2P. If MGM had taken the time to research this phenomenon first and to reach out to the OSCs involved, it is likely some sort of collaborative agreement could have been reached that would have reduced the price of music while also ensuring that positive relations were maintained, reinforcing the cultural norms (limiting P2P participation because it was viewed as stealing), and reducing the potential to create a market effect (public feels justified in pursuing free music sharing based on response of authority). Partnering would have resulted in an overall net gain instead of lost resources and damaged relations that created an anonymous file-sharing server and a great deal of mistrust with the online community.[114]

B. THE CYPHER WAR PERIOD: ZIMMERMAN, BERNSTEIN, AND JUNGER VS. US POLICY

The P2P fight was not the first time a corporate or government entity had encountered this type of regulatory challenge. History holds several pertinent examples that may have seemed like anomalies but actually formed the start of a new historical trend and of an important era in OSC history known as the Cypher Wars. During the 1990s, concerns over export and sharing of cryptographic methods led to failed regulation. This would be the start of a trend highlighting the failure of policy to keep pace with technological evolution.[115]

Government policy aimed to maintain US and UK superiority in the encryption field, an area in which these nations had dominated since World War II. Cryptographic developments were subject to review by the government under the US Munitions List

[114] Brafman and Beckstom, *Starfish and the Spider*; Samuelson, "Three Reactions"; Storch, "Down the Garden Path."

[115] Bryans, "Unlocked and Loaded"; Camp and Lewis, "Code as Speech"; Cindy Cohn, "Nine Epic Failures of Regulating Cryptography," *Deeplinks* (Blog), Electronic Frontier Foundation, September 26, 2014, https://www.eff.org/en-gb/deeplinks/2014/09/nine-epic-failures-regulating-cryptography; Michael Dobson, *From Wassenaar to Mars: Open Source Hardware, US Export Controls, and Avoiding Missteps in the Maker Movement* (N.p.: Kelley Drye, March 2015), http://www.kelleydrye.com/publications/articles/1927/_res/id=Files/index=0/wassenaar_whitepaper_v3.pdf; Levy, "Crypto Rebels"; Levy, "Cypher Wars: Pretty Good Privacy Gets Pretty Legal," *Wired*, November 2, 1994, 1–3; Storch, "Down the Garden Path."

(USML), with the goal of protecting US communications and also preventing foreign nations from gaining advanced encryption capabilities. The regulation of encryption posed a significant barrier to those working in the field by limiting the ability to share information and techniques and restricting much of the collaborative work that occurs globally in cryptography today. These restrictions led to several court cases which signaled the start of the OSC move toward greater decentralization, the use of open source to gain independence from outdated government policy, and the development of innovations leading to the exponential evolutions that challenge traditional regulation today.[116]

In 1991, Phil Zimmerman, a computer scientist and hacker, developed and released an open-source encryption package known as Pretty Good Privacy (PGP). The program was shared on Internet forums to support peace activists. It quickly spread from US users to global activists seeking secure communications tools to protect their networks from crackdowns by radical and dictatorial regimes. The USML was the primary regulatory vehicle at the time for encryption programs. Encryption software that used 40-bit keys or less was not subject to regulation, but a tool like PGP, which used a 128-bit key, was classified as military-grade encryption and subject to export controls. Zimmerman's good intentions were soon under criminal investigation for export of an encryption program without a license. In the first example of "compliance without effect,"[117] Zimmerman stopped sharing PGP online and replaced it with a published book. Anyone could purchase the book, which contained the complete text source code to create a copy of PGP. Books, unlike code, were protected by the First Amendment and not subject to regulation by the USML. The criminal investigation was eventually dropped. To avoid future regulatory issues, specifically patent and export-control trouble, Zimmerman upgraded PGP and made the code open source. PGP continued to be published in book format until export regulations were finally changed nine years later.[118]

---

[116] Bryans, "Unlocked and Loaded"; Camp and Lewis, "Code as Speech"; Cohn, "Nine Epic Failures"; Dobson, *From Wassenaar to Mars*; Levy, "Crypto Rebels"; Levy, "Cypher Wars"; Storch, "Down the Garden Path."

[117] Bryans, "Unlocked and Loaded."

[118] Levy, "Crypto Rebels"; Levy, "Cypher Wars"; Bryans, "Unlocked and Loaded."

The battle to have code recognized as protected speech under the First Amendment continued, this time at the University of California Berkley. Daniel Bernstein, a student in the mathematics department, sought to publish an academic paper on an encryption algorithm he had developed, dubbed Snuffle. Bernstein wanted to share the source code to his algorithm, but like Zimmerman, he was told the code could not be shared because it fell under the USML and the International Traffic in Arms Regulations, which was designed to keep defense-related technologies from potential adversaries. Since Snuffle was not a government project nor designed or funded for use by the government, Bernstein filed a lawsuit against the State Department protesting the restriction. The courts eventually found in favor of Bernstein. The final finding determined that source code was:

> [F]unctional language [that] deserves free speech protections, that source code is protectable speech . . . and that the ITAR licensing system as applied to Category XIII(B) [which pertains to cryptography] acts as an unconstitutional prior restraint in violation of the First Amendment . . . and is unenforceable . . .[119]

A third case began in 1996, when Peter Junger, a professor at Case Western Reserve University, was restricted to teaching a US-only class on computer law because the encryption software he used was export controlled under the USML and ITAR. Junger filed a case against the US government, and in 2000, the courts again ruled that "source code is indeed a protected, expressive means of speech secured by the First Amendment."[120]

In all three above examples, existing regulations (USML and ITAR) were unsuccessful in addressing government concerns. Broad application of policy to a complex problem set (export control), failure to address a specific security concern (lack of targeted policy), poor formulation (policy results in unequal application, leading to ineffective regulation and wasted resources), and poor execution (it was nine years before policy changed) are systemic issues that will prevent the government from successfully addressing linear technological advances, not to mention addressing the exponential

[119] See note 116.

[120] See note 116.

challenges presented by RLT. Anonymizing technologies, distrust of the government, and proliferation of disruptive technology via digital means were the end result.[121]

A more succinct illustration of exactly how traditional regulations and policy would fare when pitted against an RLT can be seen in the below table, which emphasizes the challenges of applying existing policy and regulation to 3D-printed gun designs.[122]

Table 1. Traditional Regulation of 3D-Printing Digital Design

Regulation/ Policy	**Policy Target**	**Gap**	**Outcome**
US Munitions List	Foreign nationals Physical export/import	Fails to prevent digital data or technology transfers No effect on US citizen use Ineffective in regulating technical data online Limited to import/export enforcement	Unenforceable, reactive policy leaves multiple domestic and international policy loopholes that can be exploited by nefarious actors
ITAR	Foreign nationals Physical export/import	Fails to prevent digital data or technology transfers No effect on US citizen use Ineffective in regulating technical data online Limited to import/export enforcement	Unenforceable, reactive policy leaves multiple domestic and international policy loopholes that can be exploited by nefarious actors

[121] See note 116.

[122] See note 116.

Table 1. Traditional Regulation of 3D-Printing Digital Design (cont)

Regulation/ Policy	**Policy Target**	**Gap**	**Outcome**
Undetectable Firearms Act (UFA)	US domestic users	Fails to prevent digital data or technology transfers As long as design has 3.7 oz. stainless steel/major parts are detectable by X-ray, not illegal Violations created by user who fails to adhere to CAD design are not legal responsibility of designer or producer	Applies only to legally defined firearms that violate UFA requirements; does not apply to 3D-printed metal firearms
Invention Secrecy Act	US agencies and inventors	Fails to prevent digital data or technology transfers Limited to patents	No regulatory effect on open-source 3D-printed firearms
State or City Ban	US domestic users	Fails to prevent digital data or technology transfers Violates First Amendment (ex. firearm is meant as political statement, art, model, video game design, etc.)	Potential Second and Fourth Amendment implications; poorly formulated policy leads to anonymizing behaviors, proliferation of censored materials, and cyber safe havens for bad actors
Publicly Expressed Intent to Regulate	US domestic users	Fails to prevent digital data or technology transfers	Potential First, Second and Fourth Amendment implications; poorly formulated policy leads to anonymizing behaviors, proliferation of censored materials, and cyber safe havens for bad actors

Adapted from Bryans, Danton. "Unlocked and Loaded: Government Censorship of 3D Printed Firearms and a Proposal for More Reasonable Regulation of 3D Printed Goods." Indiana Law Journal 90, no. 2 (April 2015, 2015): 901-934. Camp, Jean and Ken Lewis. "Code as Speech." Ethics and Information Technology 1, no. 2 (MAR 2001, 2001): 1-17; Dobson, Michael. From Wassenaar to Mars: Open Source Hardware, U.S. Export Controls, and Avoiding Missteps in the Maker Movement. Online: Kelley Drye, 2015; Storch, Joseph. "3-D Printing Your Way Down the Garden Path: 3-D Printers, the CopyRightization of Patents, and a Method for Manufacturers to Avoid the Entertainment Industry's Fate." New York University Journal of Intellectual Property & Entertainment Law 3, no. 2 (Spring 2014, 2014): 1-59.

These same challenges appear when considering the application of the Nuclear Regulatory Commission, Wassenaar Arrangement, Drug Enforcement Agency's export control 21 CFR Part 1312 (because certain 3D printers can manufacture drugs),[123] Export Administration Regulations, or the Commerce Control List. While many of the regulations have caveats to control and protect information, technology, or certain types of data, none of them are enforceable online. More to the point, less than 1% of those who perpetrate online crimes (such as identity theft, cyberfraud, or cyberattacks) are actually caught and prosecuted. If it is this challenging to enforce existing criminal law in cyberspace, how much more challenging will it be to enforce regulations—designed to control the physical movement of dangerous items—in a digital environment where decentralized P2P software can share encrypted files that are undetectable even when displayed in plain sight?[124]

C. POLICY PITFALLS: PHILADELPHIA'S 3D GUN BAN

The Liberator example shows just how complex the cyber/technology regulatory environment and how swift an online community response can be, especially when the state choses to take a "hard policing" approach. Even though Defense Distributed voluntarily obeyed the State Department's request, the Liberator files are still on the web, and they continue to proliferate and evolve. Attorney Danton Bryans discusses the developing culture of "compliance without effect," noting that although online and technology actors may comply with regulation requests, the digital environment and its accompanied technologies negate these actions. This is a definite challenge to traditional policy meant to address the problems of a linear, physical world. A second aspect, the "Streisand effect," further complicates the task of designing and implementing effective policy. The Streisand effect, named after Barbra Streisand's efforts to remove photos of

[123] Oliver Wainwright, "The First 3D-Printed Pill Opens up a World of Downloadable Medicine," *Guardian*, August 5, 2015, 1–2; Dominic Basulto, "Why It Matters That the FDA Just Approved the First 3D-Printed Drug," *Washington Post*, August 11, 2015, 1–4; Robinson Meyer, "3-D Printed Drugs Are Here," *Atlantic*, August 19, 2015, 1–4.

[124] Dobson, *From Wassenaar to Mars*; Estes, "Getting Better and Scarier"; Paul, "'Disarming Corruptor'"; Soska and Christin, "Measuring the Longitudinal Evolution"; Federal Bureau of Investigation, Internet Crime Complaint Center. 2011 Internet Crime Report. N.p.: Internet Crime Complaint Center, 2011; Federal Bureau of Investigation, Internet Crime Complaint Center. 2014 Internet Crime Report. N.p.: Internet Crime Complaint Center, 2014.

her private beach home from the web, occurs when policy dictates that information be removed from the digital environment or tries to restrict access. When this happens, actions taken have the opposite effect and result in widespread proliferation. In the case of Defense Distributed, the State Department's intent was to limit access to the files and prevent proliferation. Today, the Liberator has been joined by an increasingly diverse array of 3D weapon designs, the exact opposite of the desired end state.[125]

Reactive policy is another serious pitfall. In 2013, the City of Philadelphia announced a pre-emptive policy outlawing all 3D-printed guns. Citizens were notified that they were not allowed to 3D print any gun in whole or in part. With this policy, Philadelphia opened itself to a resource intensive, unenforceable legal quagmire. How will the city know if a citizen has a 3D printer? How will it know if the citizen has downloaded a 3D weapon file for a printer or actually printed a gun or gun parts? Bill no. 130584 offers no details on how this ordinance will be enforced. What will the punishment be? Will it be different for juveniles than for adults? What about 3D-printed guns used in jewelry, in artwork, or as a political statement? Will this broad policy open the city up to a barrage of lawsuits?[126] The policy failed as soon as it was announced. It was reactive and developed in response to a perceived threat, one that may not have even existed within the city. The application of broad policy vice a targeted policy shows a lack of understanding, making it ineffective and unenforceable, with the potential to generate a number of legal battles. A third failure point is that no one with subject-matter expertise was involved in crafting this policy. A lack of understanding of an RLT when

---

[125] Bryans, "Unlocked and Loaded"; Greenberg, "Feds Tighten Restrictions"; "The Economist Explains: What is the Streisand Effect?" *Economist*, April 15, 2013, 1, http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-what-streisand-effect.

[126] Bryans, "Unlocked and Loaded"; Dobson, *From Wassenaar to Mars*; Estes, "Getting Better and Scarier"; Paul, "'Disarming Corruptor'"; Worstall, "Philadelphia Passes Law"; Addy Dugdale, "Philadelphia is the First City to Ban 3-D-Printed Guns," *Fast Company*, November 25, 2013, http://www.fastcompany.com/3022195/philadelphia-is-the-first-city-to-ban-3-d-printed-guns; Stephen Gutowski, "Pioneer of 3D-Printed Guns Explains Why He's Suing the State Department," *Washington Free Beacon*, July 8, 2015; Lucas Mearian, "U.S. State Department Moves to Block 3D-Printed Gun Plans Online," *ComputerWorld*, July 7, 2015; Simon Van Zuylen-Wood, "Philly Becomes First City to Ban 3-D Gun Printing," *Philadelphia*, November 21, 2013; Whitwam, "U.S. State Department Begins"; "First Ban in the Country: 3D-Printed Guns Now Illegal in Philadelphia," *Russia Today*, November 25, 2013, https://www.rt.com/usa/philly-gun-ban-johnson-280/.

developing policy means that the OSCs involved are more likely to reject that policy, to anonymize, and to work successfully against any enforcement attempts.[127]

A much more effective approach would have been to work with local OSC members to craft a smart policy that considered the technology and focused on those specific areas of concern to public safety. Partnering with public and private subject-matter experts does several things: it creates open communications channels, builds trust, gets buy-in, and results in policy that will actually work, because the people who are regulated by it helped to create it. Partnering also prevents conflict between government and technology drivers and users, another challenge that is becoming more common in the policy arena.[128]

D. LIGHTSQUARED: TECHNOLOGY VS. THE GOVERNMENT

In 2004, mobile communications venture company LightSquared developed, applied for, and was approved to operate a 4G LTE network within the US. The company decided to modify the network setup to include a series of ground stations. The problem with the new setup came when LightSquared ground stations began to interfere with federal government Global Positioning System (GPS) receivers, most significantly those owned by the military under Air Force Space Command. The company had been told that they must resolve any interference issues, but LightSquared pushed ahead without a mitigation plan. The issue was brought before Congress. Air Force General William L. Shelton testified that after extensive research, no mitigation options had been found that would allow the military GPS receivers and the LightSquared network to effectively

[127] Worstall, "Philadelphia Passes Law"; Dugdale, "Philadelphia Is the First City"; Gutowski, "Pioneer of 3D-Printed Guns"; Mearian, "U.S. State Department Moves"; Van Zuylen-Wood, "Philly Becomes First City"; Whitwam, "Banning 3D Printed Guns Online"; *Russia Today*, "First Ban in the Country"; Bryans, "Unlocked and Loaded"; Dobson, *From Wassenaar to Mars*; Estes, "Getting Better and Scarier"; Paul, "'Disarming Corruptor'"; Soska and Christin, "Measuring the Longitudinal Evolution."

[128] Worstall, "Philadelphia Passes Law"; Dugdale, "Philadelphia Is the First City"; Gutowski, "Pioneer of 3D-Printed Guns"; Mearian, "U.S. State Department Moves"; Van Zuylen-Wood, "Philly Becomes First City"; Whitwam, "Banning 3D Printed Guns Online"; *Russia Today*, "First Ban in the Country"; Dobson, *From Wassenaar to Mars*; Estes, "Getting Better and Scarier"; Paul, "'Disarming Corruptor'"; Soska and Christin, "Measuring the Longitudinal Evolution."

coexist. LightSquared went bankrupt, and the Air Force GPS receivers went back to work.[129]

While the problem was solved, the resolution was far from satisfactory to all parties. Conflicts that result in failed enterprises like LightSquared mean that future private technological endeavors may be built explicitly to avoid interaction with the government. This will not be the last battle to occur between government and technology, and as noted in a recent *Air Force Magazine* article, "it was unsettling to see a business plan boldly pitted against national security requirements and a fight driven by investor interests."[130]

As demonstrated by these first case studies, there is much work to be done. The US appears poorly organized to deal with regulation in an exponential environment. Policy itself is one part of the solution, but the government also needs to be able to effectively partner with highly dynamic innovative organizations, a difficult task for a hierarchical, linear structure.[131] Conflict will continue between government and innovators as long as the two remain separated by processes, cultural differences, language, and a lack of effective partnerships.[132] Indifference, lack of incentive to work with government entities, and the ability and resources to move ahead without a

---

[129] Ben FitzGerald and Kelley Sayler, *Creative Disruption: Technology, Strategy and the Future of the Global Defense Industry* (Washington, DC: Center for a New American Security, 2014), http://www.cnas.org/sites/default/files/publications-pdf/CNAS_FutureDefenseIndustry_FitzGeraldSayler.pdf; Rebecca Grant, "The Silicon Offset," *Air Force Magazine*, March 2015, 44–48; Phil Goldstein, "LightSquared Could Target First Responders, Transport and Energy Industries with New Service," *FierceWireless,* April 8, 2015, http://www.fiercewireless.com/story/lightsquared-could-target-first-responders-transport-and-energy-industries/2015-04-08; Goldstein, "LightSquared Hires Advisers to Help Overcome GPS Industry Concerns," *FierceWireless,* June 30, 2015, http://www.fiercewireless.com/story/lightsquared-hires-advisers-help-overcome-gps-industry-concerns/2015-06-30; Arthur Herman, "Obama vs. GPS," *National Review*, September 21, 2011; Stephen Lawson, "LightSquared vs. GPS Raises Big Spectrum Issues," *PCWorld*, July 25, 2011, 1–7; Steven Musil, "FCC Suspends LightSquared Waiver over GPS Interference," *CNET*, February 14, 2012, 1; *Sustaining GPS for National Security, Hearing before the Subcommittee on Strategic Forces of the Committee on Armed Services, Hours of Representatives*, 112th Cong. (2011) (statement of General William L. Shelton, Commander, Air Force Space Command).

[130] Grant, "Silicon Offset."

[131] John Arquilla, "To Build a Network," *Prism* 5, no. 1 (September 2014): 23–33, http://www.ndu.edu/Portals/59/Documents/CCO/PRISMVol5No1.pdf; Briggs and Shingles, "Exponentials"; FitzGerald and Sayler, *Creative Disruption*; Phil Williams, "The Nature of Drug-Trafficking Networks," *Current History* 97, no. 618 (April 1998): 154–59.

[132] Grant, "Silicon Offset"; Herman, "Obama vs. GPS"; Lawson, "LightSquared vs. GPS"; FitzGerald and Sayler, *Creative Disruption*.

government partner provide innovators a great deal of leverage. It is doubtful that once such an evolution takes place the government will be able to catch up via existing bureaucratic processes. It would be like a motorhome trying to catch a Tesla, and likely as successful.[133]

These five case studies illustrate some of the challenges for regulators working within the RLT space. None of this is life threatening at this time; that may not be the case three years from now. Exponential advancements are making RLT more accessible, and the number of dangerous incidents reported is also exponentially increasing: effective drone employment by non-state actors against nation-states; computer hacks that control boats, trains, and planes; 3D-printed illicit drug sales; synthetic biological organisms; and battlefield robot snipers all seem like plotlines for some wild science fiction story, but all of these events have already occurred.[134]

In the next section, five case studies showing progress in the area of RLT and OSC collaboration will be examined. In each case, specific actors came together with government or corporate agencies to make a positive difference. These cases demonstrate the power such partnerships can have when facing exponential challenges. The case studies include the Federal Bureau of Investigation (FBI) and DIY biohackers partnership, Department of Homeland Security (DHS) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Finest Squad vs. Lizard Squad as an example of cyber self-policing, hacktivist group Anonymous's voluntary support to counterterrorism efforts against ISIS, and the DHS San Diego Law Enforcement Coordination Center (SD-LECC) fusion center agreement with the San Diego InfraGard Members Alliance (IMA) as a successful example of a formalized partnership with

---

133 Grant, "Silicon Offset"; Herman, "Obama vs. GPS"; Lawson, "LightSquared vs. GPS"; Musil, "FCC Suspends LightSquared Waiver."

134 Siryoti, "Iran Admits Hezbollah's Drone"; Ali Hashem, "Assassinated Hezbollah Leader Key to Technology, Drone Operations," *Al-Monitor*, December 4, 2013, http://www.al-monitor.com/pulse/originals/2013/12/hezbollah-assassinated-hashem.html; Isabel Kershner, "Israel Shoots down Drone Possibly Sent by Hezbollah," *New York Times*, April 25, 2013; Goodman, "Crime Has Gone High-Tech"; Goodman, *Future Crimes*; Wainwright, "First 3D-Printed Pill"; Basulto, "Why It Matters"; Meyer, "3-D Printed Drugs Are Here"; Philip Ross, "'Printing' Alien Life? Geneticist Craig Venter Says 3D Printers Could Recreate Martian DNA on Earth," *International Business Times*, October 7, 2013, 1–2; Venter, "First Self-replicating Synthetic Bacterial Cell."

public- and private-sector actors to meet homeland-security and disaster-preparedness requirements.[135]

E. THE FBI AND BIOHACKING: BUILDING A CULTURE OF SHARED SECURITY VALUES

Partnering with actors at the leading edge of RLT development and employment is one way to keep pace with developments in this area, and it has paid tremendous dividends in the growing field of biohacking and synthetic biology. As the movement became more popular, concern over the lack of standardized safety protocols and regulation led security experts to advocate for a new strategy to limit potential risks. The FBI decided to start an outreach program to biohacking groups to discuss security concerns and advocate for ethical and responsible biology standards. Special Agent You, lead for the outreach effort, used his prior experience as a gene therapist to set up a series of biosecurity conferences and informal meetings across the nation to introduce the FBI, US Department of Health and Human Services, and State Department to this OSC. At first the groups were hesitant about the government's involvement, but fears quickly dissipated when government representatives voiced their goal: "to build common cause on efforts to support research while raising awareness of security issues."[136] Researchers, hobbyists, biotech firms, and government policymakers began to work together to balance the potential risks and benefits of these cutting-edge developments, guaranteeing

---

[135] Lempinen, "FBI, AAAS Collaborate"; Kenrick Vezina, "Culture Wars Threaten Synthetic Biology's Future: Debate on Open Source Versus Closed Door," *Genetic Literacy Project*, May 9, 2014, http://www.geneticliteracyproject.org/2014/05/09/culture-wars-threaten-synthetic-biologys-future-debate-on-open-source-versus-closed-door/; Anthony Cuthbertson, "Anonymous Affiliate GhostSec Thwarts ISIS Terror Plots in New York and Tunisia," *International Business Times*, July 22, 2015, 1–3, http://www.ibtimes.co.uk/anonymous-affiliate-ghostsec-thwarts-isis-terror-plots-new-york-tunisia-1512031; Parker Scott, "The FBI's InfraGard Program," presentation, InfraGard San Diego Members Alliance, July 20, 2012, http://www.infragardsd.org/docs/isd-ppt.pdf; Adam Stone, "National Fusion Center Model Is Emerging," *Emergency Management*, January 23, 2015, 1–3; Matthew Miller, "Formalizing Fusion Center Public and Private Sector Partnerships, A Practical Model," San Diego Law Enforcement Coordination Center & San Diego InfraGard Member Alliance White Paper, March 2015.

[136] Andrew Hessel, Marc Goodman, and Steven Kotler, "Hacking the President's DNA," *Atlantic*, November 2012, 1–29; Scott Leibrand, "How and Why We Are Working with the FDA: Background and a Brief Summary of the Recent Meeting with the FDA about the Nightscout Project," *DIYPS.org*, October 12, 2014, http://diyps.org/2014/10/12/how-and-why-we-are-working-with-the-fda-background-and-a-brief-summary-of-the-recent-meeting-with-the-fda-about-the-nightscout-project/; Lempinen, "FBI, AAAS Collaborate"; You, Edward H. "FBI Perspective: Addressing Synthetic Biology and Biosecurity." Presentation. Presidential Commission for the Study of Bioethical Issues, Washington, D.C., July 9, 2010.

innovation while protecting public safety by setting effective standards to prevent ignorant or illicit use of these technologies.[137]

Government officials had reason to be concerned. The 2001 anthrax attacks and the successful mail-order purchase of smallpox by the *Guardian* meant existing biotechnology regulations were falling short. In an effort to close the gaps, federal agents aggressively interviewed academics, researchers, and biotech firms to find a viable solution. But this approach caused the biotech community, including analysts working for the FBI, to feel mistrusted, ostracized, and isolated. Kavita Berger, associate program director for the Center for Science, Technology, and Security Policy, conducted a poll of researchers following the government interviews. The results, as far as promoting a cooperative, collaborative information-sharing environment, were abysmal. The federal approach had created a more closed, suspicious, fearful group of individuals who were now less likely to reach out to law enforcement. The lack of an open, transparent relationship meant that efforts to improve security would be limited at best. Policy implemented from these efforts would likely fail or make the situation worse by imposing regulations that hindered legitimate science but had little impact on improving security.[138] Berger noted, "[Collaboration is] ultimately going to be a lot more productive and a lot more useful in reaching the end goals of security and science."[139]

In large part, the FBI outreach initiative is responsible for turning this situation around. The end result is a series of collaborative partnerships that has led to substantial improvements in biosecurity by identifying gaps and potential threats. The initiative is a solution incubator, providing policymakers with the subject-matter expertise critical to improving security. Policymakers gain a true understanding of technological capabilities

---

[137] Hessel, Goodman, and Kotler, "Hacking the President's DNA"; Leibrand, "Working with the FDA"; Lempinen, "FBI, AAAS Collaborate."

[138] Charisius, Friebe, and Karberg, "Becoming Biohackers"; Hessel, Goodman, and Kotler, "Hacking the President's DNA"; Federal Bureau of Investigation, "Amerithrax or Anthrax Investigation," accessed March 5, 2015, https://www.fbi.gov/about-us/history/famous-cases/anthrax-amerithrax; Joby Warrick, "FBI Investigation of 2001 Anthrax Attacks Concluded; U.S. Releases Details," *Washington Post*, February 20, 2010: 1–2; James Randerson, "Did Anyone Order Smallpox?" *Guardian*, June 23, 2006, 1; Leibrand, "Working with the FDA"; Lempinen, "FBI, AAAS Collaborate."

[139] Hessel, Goodman, and Kotler, "Hacking the President's DNA"; Leibrand, "Working with the FDA"; Lempinen, "FBI, AAAS Collaborate"; Vezina, "Culture Wars Threaten."

and how to best address challenges. A secondary benefit has been the development of mutual respect and a culture of shared values between the federal government and the biohacking OSCs.[140] Ellen Jorgensen, president of Genspace, a community lab in New York City, highlighted the benefit of partnering as seen from the OSC side.

> I think that the meetings we have had were very useful in terms of fostering some trust between the FBI and the DIYBio community. . . . We are all arriving at the same place, it seems, dragged kicking and screaming into more organization than we thought we'd be comfortable with in the beginning. But if a system of safety standards, operating procedures, advisory committees, and training records for lab members will allow us to get on to the good stuff and do science instead of just talking about it, it's a small price to pay.[141]

The FBI's outreach is one example of an effective approach to threat mitigation. When asked his thoughts on the outreach program, Special Agent You acknowledged the benefits to both DIYBio and the FBI:

> We've started building these bridges and we have a real commitment to understanding this community and a real appreciation . . . the reason the FBI is reaching out to DIY biology groups is not because there's a threat . . . but because we want to make sure it's done safely and securely.[142]

The FBI–DIYBio collaboration provides some important takeaways for government members involved with RLT. Partnering with an OSC grants policymakers and regulators access to valuable insights and subject-matter expertise necessary to create effective policy. DIYBio, as an informed partner, also benefits by understanding the government's safety and security concerns and works internally to mitigate those concerns. The OSC can conduct activities openly, with no need for anonymizing technology, which in turn aids preventing threat-actor exploitation. Since the development of this partnership, DIYBio has stepped up efforts to emphasize a culture of ethical, responsible science embedded in the group's cultural norms. This is a powerful tool in protecting against abuse. For these groups, science is everything. It is a chance to make the world a better place. DIYBio will not jeopardize that by willfully performing

---

[140] Lempinen, "FBI, AAAS Collaborate"; Vezina, "Culture Wars Threaten."

[141] Lempinen, "FBI, AAAS Collaborate."

[142] Ibid.

science that threatens public safety and security. Finally, a network of self-policing groups now exists with the expertise to detect and identify illicit, dangerous actions or limit the access of potential nefarious actors to the free expertise offered by these OSCs. The cost of the outreach program is low. Fewer than a hundred FBI agents actively engage with the DIYBio community to promote continued information sharing and open discussion. Developing a parallel network with the access and expertise required to monitor and regulate a global OSC would cost millions of dollars, while the impact of such an endeavor would be minimal. The end result would be ineffective policy and reactive threat response instead of the proactive, innovative, cost-effective approach that exists today.[143]

F. THE BATTLE FOR CRITICAL INFRASTRUCTURE SECURITY: DHS AND ICS-CERT

The Internet is one of the most powerful Radical Leveling Technologies in existence. A tremendous source for innovation, the Internet is also a vehicle for disruption and destruction. One area of concern is targeted attacks against critical infrastructure. To find agile solutions that can match the decentralized, hybrid efforts of cyberattackers against infrastructure targets, the Department of Homeland Security built a collaborative partnership with various OSCs to enhance its capabilities in this area. The Industrial Control Systems Cyber Emergency Response Team was created for just this purpose. The mission of ICS-CERT is "to reduce risks within and across all critical infrastructure by forming a partnership with law enforcement agencies and the intelligence community and coordinating efforts among federal, state, local, and tribal governments and control system owners, operators, and vendors."[144] ICS-CERT is a 24/7 reach-back and emergency-response capability that relies on OSCs to provide cyber-situational awareness and immediate onsite incident response around the globe. ICS-CERT also provides free training, diagnostics software, malware intelligence, threat

[143] Hessel, Goodman, and Kotler, "Hacking the President's DNA"; Leibrand, "Working with the FDA"; Lempinen, "FBI, AAAS Collaborate"; Vezina, "Culture Wars Threaten."

[144] Sandra Jontz, "Critical Infrastructure Is Cyberterrorism's Next Likely Target," *Signal*, March 2015, 18–21; Pierluigi Paganini, "ICS-CERT MONITOR Report States Most Critical Infrastructure Attacks Involve APTs," *Security Affairs* (blog), March 6, 2015, http://securityaffairs.co/wordpress/34936/cyber-crime/ics-cert-monitor-report-apt.html.

briefings, and vulnerability assessments to critical infrastructure owners and operators, allowing a proactive approach to threat management. Via alerts and advisories, ICS-CERT provides valuable, timely information on the digital environment.[145] Frank Mong, vice president and general manager of solutions for Hewlett-Packard and ICS-CERT collaborator, highlighted why a networked structure like ICS-CERT is so important to critical infrastructure community members:

> The adversary is an ecosystem. . . . It's very hard for us to pinpoint a specific actor, and what we find is that the threat actors have organized, and they're working together. So whether they're cyber-criminal gangs to nation-states or hacktivists, they're all collaborating and are very specialized. Some are very good at doing certain things and they can sell that specialization to somebody else with a particular intent or a particular project or plan. We're talking an entire marketplace, an entire ecosystem of highly specialized, highly talented people who have the ability to do a lot of different things.[146]

Examples like ICS-CERT demonstrate how a hybrid approach to security can conserve resources, streamline processes, and produce successful policy solutions. In this case, ICS-CERT is the government's initial attempt to employ a decentralized OSC network of expertise and capabilities to address the exponential effects of the cyber realm. By building a network to beat a network, ICS-CERT is able to proactively confront threats and surge support to sites that need it most. DHS efforts to boost early warning by teaming with OSCs and private industry is a study in how to crowdsource intelligence. Along with increased agility, the organization relies on a small footprint; in 2015, it operated on a budget of $8.5 million while supporting 1,600 customers.[147] This includes classified outreach conducted at the Secret level to share actionable information with community members nationwide.[148]

---

145 "ICS-CERT Monitor Spring 2013," Department of Homeland Security, 2013.

146 Jontz, "Cyberterrorism's Next Likely Target."

147 Ibid.; John Arquilla, "The New Rules of War," *Foreign Policy*, February 11, 2010, 1–16, http://foreignpolicy.com/2010/02/11/the-new-rules-of-war/; "ICS-CERT Monitor 2015," Department of Homeland Security, 2015; "ICS-CERT Monitor 2014 Fiscal Report," Department of Homeland Security, 2015.

148 Department of Homeland Security, "ICS-CERT Monitor 2014 Fiscal Report."

ICS-CERT is a solid initial concept, but there is still work to be done. Intelligence shortfalls and coordination issues persist due to bureaucratic stovepipes that hamper interagency sharing.[149] Fusion centers will need to move away from linear processes and structure and embrace the fluid, dynamic nature of OSC culture in order to keep pace with exponential evolution.[150] ICS-CERT partnership with online community members will improve the initial capacity and expertise at little to no cost. This will also provide the capabilities necessary to revise existing policy or craft new policy, allowing the organization to stay at the leading edge when addressing infrastructure threats. Another option is the creation of a cyber-bounty program, which would increase proactive efforts to identify security breaches. This should be the focus of the next ICS-CERT outreach to OSCs, in order to garner the support of hackers who understand and are willing to collaborate on infrastructure security issues.[151]

Organizations like ICS-CERT are helpful as an intermediate bridge between formal government processes and functioning successfully in a faster technological environment. However, in certain cases, a much more decentralized approach is required and may in fact be the only viable solution. Corporate tech giants Sony and Microsoft are multibillion-dollar enterprises who fight and lose regularly to malicious actors targeting the computer and gaming industries. As we have seen, conventional cybercrime units cannot keep pace with digital natives. Malicious actors on the net are a minority, but they perpetrate a large number of crimes and are difficult to stop. Yet there have been a number of instances in which hackers have conducted self-policing efforts to stop those who defy online norms for nefarious purposes. One of the harshest reactions to a violation of netiquette is doxing (publically posting personal information identifying an

---

149 Brian Krebs, "DHS Blasts Reports of Illinois Water Station Hack," *Krebs on Security* (blog), November 22, 2011, http://krebsonsecurity.com/2011/11/dhs-blasts-reports-of-illinois-water-station-hack/; Ellen Nakashima, "Water-Pump Failure in Illinois Wasn't Cyberattack after All," *Washington Post*, November 25, 2011, 1; Paganini, "Infrastructure Attacks Involve APTs"; Kim Zetter, "DHS Issued False 'Water Pump Hack' Report; Called it a 'Success,'" *Wired*, February 10, 2012, 1–13.

150 Thomas Fox-Brewster, "Hundreds of Wind Turbines and Solar Systems Wide Open to Easy Exploits," *Forbes*, June 12, 2015, 1–3, http://www.forbes.com/sites/thomasbrewster/2015/06/12/hacking-wind-solar-systems-is-easy/.

151 loldhs pr0f, "City of South Houston SCADA Vulnerabilities," *Grid: A Digital Frontier* (blog), November 18, 2011, http://pastebin.com/Wx90LLum.

individual online), which typically results in severe harassment from members of the online community and a visit from police or federal authorities, depending on the nature of the violations. These actions maintain balance and prevent nefarious actors from wreaking havoc online.

G. FINEST SQUAD: HACKERS DEFEATING BOT-THUGS WITH CYBER SELF-POLICING

In 2014, a hacker gang called Lizard Squad was in the news following attacks on Sony's PlayStation gaming network and Blizzard's popular World of Warcraft servers and for posting a bomb threat online targeting Sony executive John Smedley. While hacking game servers and disrupting service is sometimes acceptable if meant as a brief prank or to highlight vulnerabilities, Lizard Squad made their new mission the takedown of the Sony PlayStation network and Microsoft's Xbox network for the entire month of December. Lizard Squad even announced their plans online and notified Sony and Microsoft of their intent. Despite the advance warning, neither corporation was able to stop the attack.[152]

In response to public outcry over the holiday attacks, a hacker group called Finest Squad decided enough was enough. Working online, the group discovered and revealed Lizard Squad's members through various social media accounts, releasing their home addresses, photos, and information to the public and the police. Finest Squad also highlighted Lizard Squad's tactics, a set of hacking tools costing less than $300 that targeted specific security flaws in both corporations' networks and could take out the servers using a massive denial of service (DDos) attack. This information was shared with both Sony and Microsoft so that fixes could be made. Following the arrests of the Lizard Squad, additional information revealed the attacks were conducted to advertise the group's new DDos tool, Lizard Stressor, which the group had been selling online.

[152] Cook, "Hacker Gang Literally Saved Christmas"; RFSID, "Lizard Squad."

Though Finest Squad may have prevented future attacks against PS4 and Xbox, it is likely that Lizard Stressor may appear again, used by other groups against new targets.[153]

This is one example of many in which groups or individuals have self-policed or provided aid to law enforcement in order to stop online crimes. These are important aspects of the online culture that policymakers need to consider. Incorporating OSCs into the policy-development process and inviting them to partner (formally or informally) with law enforcement and intelligence will ensure the Internet is kept open, safe, and secure while also building capacity, access, and expertise to identify and stop potential future threats.[154]

H. HACKTIVISM: HOW GROUPS LIKE ANONYMOUS ARE HELPING TO IMPROVE SECURITY

Many find it surprising that Microsoft, a major cybersecurity software provider, was defeated by a small group of bad actors using tools that cost less than $500. But this is the impact of RLT: the ability to create leverage and change the balance of power in unanticipated ways. Malicious actors understand that digital networks grant them an edge against the government. The lack of a credible threat to these actors is the reason for the continued increase in cybercrime. Though the government is aware of the issues, several hacktivist groups have determined the government is ineffective or, due to restrictive rules and hierarchical bureaucratic structures, insufficiently agile to address many developing technological threats. The hacktivist group Anonymous is one example. Anonymous is often confusing to those attempting to understand it and its intentions. The challenge comes from the perception that this is a longstanding cohesive group, when in fact Anonymous is a collective, an assembly of individuals that form temporarily to accomplish shared goals, then splinter and move on to other projects. Members are diverse in their beliefs, backgrounds, and reasons for participation. Some choose to the

153 Cook, "Hacker Gang Literally Saved Christmas"; RFSID, "Lizard Squad"; Dylan Love, "Why Microsoft and Sony Couldn't Stop Lizard Squad Attack Despite Warnings," *International Business Times*, December 30, 2014, 1–9; William Turton, "Lizard Squad's Xbox Live, PSN Attacks Were a 'Marketing Scheme' for New DDoS Service," *Daily Dot*, December 30, 2014, http://www.dailydot.com/crime/lizard-squad-lizard-stresser-ddos-service-psn-xbox-live-sony-microsoft/.

154 Cook, "Hacker Gang Literally Saved Christmas"; RFSID, "Lizard Squad."

hack the government, while others work alongside. In many cases, government hacks come with a message highlighting security shortfalls or proclaiming a political position, or sometimes they are simply pranks. Considering these types of actors, there is no doubt that John Arquilla and David Ronfeldt's prescient thoughts on networks and netwar are in play today.[155]

Terrorism, including online aspects of terror networks, continues to be a challenge globally. Neither law enforcement nor the military is agile enough or has the internal expertise to effectively compete with the multitude of hackers and online affiliates providing support to groups like Islamic State (IS). In fact, IS was clearly dominating the net while national efforts made little permanent progress. In March 2015, that began to change as IS was confronted not by a state actor but by a unified front of hacktivists. Anonymous, GhostSec, and CtrlSec began collaborating to identify and track members of IS online. It is unheard of for these three groups to collaborate on such a large scale, but all three are agreed that this effort will protect the public and help defeat a dangerous radical element. To date, Anonymous has disrupted over a thousand IS emails, websites, and virtual private network (VPN) connections, while GhostSec has reported deletion of 57,000 IS-related accounts. Anonymous also called on the public for support. The hacktivists identified Twitter as central to the IS cyber effort and described how the IS system could be dismantled by removing this node. Anonymous solicited the public to convince Twitter to shut down the IS accounts. GhostSec also provided critical intelligence to authorities concerning a potential IS threat. Those authorities used the information to disrupt planned attacks in Tunisia and New York City.[156]

Employing digital natives in the fight against malicious actors who pose a clear and present threat to the public is a smart next step in addressing the limitations of current

---

[155] Anonymous, "FBI Using Information"; Arquilla, "To Build a Network"; Arquilla, "New Rules of War"; Cuthbertson, "Anonymous Lists 9,200 Twitter Accounts"; Arquilla, John and David Ronfeldt. Networks and Netwars: The Future of Terror, Crime, and Militancy. Santa Monica, CA: RAND Corporation, 2001; David Gilbert, "FBI Using Information from Anonymous to Help Find US Central Command Hackers," *International Business Times*, January 20, 2015; Vandita, "Anonymous Takes down ISIS Websites"; Phil Williams, "Nature of Drug-Trafficking Networks."

[156] Cuthbertson, "GhostSec Thwarts ISIS Terror"; Anonymous, "FBI Using Information"; Cuthbertson, "Anonymous Lists 9,200 Twitter Accounts"; Gilbert, "FBI Using Information"; Vandita, "Anonymous Takes Down ISIS Websites."

regulations and established structures. Anonymous affiliates have provided valuable assistance to the FBI and other organizations like US Central Command. While these groups certainly have individual agendas, there are also shared agendas that can result in a collaborative partnership on specific or limited goals. A group like GhostSec, with a stated mission "to eliminate the online presence of Islamic extremist groups such as Islamic State, Al-Qaeda, Al-Nusra, Boko Haram, and Al-Shabaab in an effort to stymie their recruitment and limit their ability to organize international terrorist efforts," presents a unique opportunity to partner with a group structured to succeed against terror online. Cyber bounties could be used to garner additional support from such groups and to focus capacity toward a specific problem set, a way to build an OSC-based netwar capability to improve public safety and security. This would be similar to the recruitment of groups like the Northern Alliance for support against the Taliban, except with one major difference: the Northern Alliance held expertise and authority only for Afghanistan. Groups like GhostSec operate as part of a transnational, decentralized network, meaning they have access to the digital environment around the globe and can conduct operations worldwide, keeping the nation ahead of the threat.[157]

I. EXPONENTIAL EFFECTS OF DIGITAL PARTNERS: DHS AND THE SD-LECC MODEL

The only way to prepare for exponential threat vectors produced by RLT is to link into the web as well. Partnering with digital natives is of proven value. However, it is still important to have intermediary structures that can liaise with both big government and the decentralized actors online. The DHS San Diego Law Enforcement Coordination Center fusion center is just such a structure. SD-LECC is an effective and functional solution for the city's law enforcement needs. The memorandum of understanding (MOU) with the San Diego InfraGard Members Alliance (IMA) is a good template for creating a formalized partnership with OSC and private-sector actors to meet homeland-security and disaster-preparedness requirements. Similar to the ICS-CERT model, San

157 "Ghost Security," Ghost Security, accessed August 15, 2015, http://www.ghostsec.org/; Arquilla, "To Build a Network"; Arquilla, "New Rules of War"; Phil Williams, "Nature of Drug-Trafficking Networks."

Diego's fusion center began as a means to protect critical infrastructure, but as the regional IMA groups began to grow, an InfraGard National Members Alliance (INMA) was established with 40,000 members, each belonging to a nonprofit organization affiliated with the FBI. This collaboration has evolved the IMA mission to include cyber, criminal, terror, and national security threats. Recent successes by the San Diego IMA highlight just how effective this organization is. Tips on terror activity, major crimes, and cyber threats are received regularly. The subject-matter expertise brought to bear by these groups is a powerful tool in countering exponential effects and keeping pace with cybercrime. The IMA groups participate in homeland-security exercises and provide insight into how attacks may be conducted, methods to detect and prevent such attacks, and how to improve system resiliency and attribution methods.[158]

In 2012, Dr. Gary Warner, a professor at the University of Alabama and InfraGard member, used data-mining tools to uncover a money-mule scheme by hackers in Eastern Europe. In one of the largest cybercrime cases to date, Warner helped FBI agents track and identify hackers and their money mules across the US by identifying the spread of the key logger the hackers were using and tracking it back to its source. Warner's students used the tools from their class to identify the remaining mules within the US, resulting in the arrest of all but one individual. Operation Trident Beach stopped hackers from getting away with almost $70 million they had stolen online. The ability of Dr. Warner and his students to operate autonomously and use open-source tools, unlimited by government requirements affecting law enforcement and military operators acting in a public space, demonstrates the power that leveraging OSC actors can have to enforce existing laws online.[159]

---

158 Amylynn Errera, "InfraGard Partnership for Protection Program Overview," Federal Bureau of Investigation, Washington Field Office, 2014; Scott, "FBI's InfraGard Program"; Stone, "National Fusion Center Model"; Miller, "Public and Private Sector Partnerships."

159 James Craig, Michael Eubanks, and Gary Warner, "CKN-3: Operation Trident Breach - Lessons Learned from FBI Global Cyber Crime Arrests," proceedings of the FOSE Conference and Exposition, Washington, D.C., July 19–21, 2011; Brian Williams, "University Professor Helps FBI Crack $70 Million Cybercrime Ring," *Rock Center NBC News*, March 21, 2012, http://rockcenter.nbcnews.com/_news/2012/03/21/10792287-university-professor-helps-fbi-crack-70-million-cybercrime-ring.

The above case studies highlight some important features of the digital landscape that can assist in developing strong policy, improving enforcement, and enhancing national security and public safety. The government can stay at the leading edge of RLT by crafting strategy grounded in the digital environment which grants it the ability to evolve as technology evolves. Such a move requires adopting a network perspective that can take advantage of the same strengths that transnational illicit networks use to defeat physical, legal, and geographic boundaries. It will require new structures to match developing decentralized networks and organizations that are equipped to compete in a networked world. Policy and law enforcement must evolve to become borderless as well. This will reduce regulatory complexity while allowing joint international efforts to leverage laws that are not limited by jurisdictional differences. And OSCs must be a cornerstone to all of these efforts in order to ensure success.[160]

These basic steps are the foundation necessary for constructing a successful strategy to deal with RLT. Developing organizational capabilities, understanding specific technologies and the implications each brings, and adopting new tactics, techniques, and procedures will enable the government to function competitively in an exponential environment where networks hold sufficient power to challenge nations.[161]

[160] Briggs and Shingles, “Exponentials”; Phil Williams, “Nature of Drug-Trafficking Networks.”

[161] Arquilla, "The New Rules of War"; Arquilla, "To Build a Network."

THIS PAGE INTENTIONALLY LEFT BLANK

V. A FLEXIBLE SPECTRUM FOR END-GAME SUCCESS

> The Air Force's ability to continue to adapt and respond faster than our potential adversaries is the greatest challenge we face over the next thirty years.
>
> General Mark A. Welsh, USAF chief of staff, *America's Air Force: A Call to the Future*, 2014

In the increasingly intertwined environment of cyber and the physical world, creating policy for emerging disruptive technologies that are evolving at an exponential rate will now be a common challenge. Radical Leveling Technologies will materialize suddenly, producing generational leaps with transnational impacts. The ability of these technologies to move from obscure, nascent concepts into mature drivers of disruption demands that policymakers approach these challenges with finesse and a solid understanding of the risks and benefits each will pose.[162]

So far, this thesis has provided insight into the revolutionary technology changes occurring today, the open-source cultures intertwined with their evolution, and some of the key challenges facing policymakers and regulators. The goal of this final chapter is to provide a potential spectrum of solutions that can form the basis of a new approach to improving international security while still encouraging innovation. A discussion of the four primary policy pitfalls will be followed with a brief exploration into potential deterrence options, at which point the paper will transition into a presentation of a foundational model (fairly basic in nature, to ensure potential for agility and flexibility) with the final goal of providing a framework that can evolve with the RLT class of technologies. The focus of this model is to prevent ignorant or malignant employment of any RLT. Thus, the final piece will provide policymakers, military, and law enforcement entities with initial recommendations on proactive defensive, offensive, and crises-response options.

---

[162] Briggs and Shingles, "Exponentials"; Davis, Nacht, and Lehman, *Strategic Latency and World Power*; FitzGerald and Sayler, *Creative Disruption*; Grame P. Herd, Detlef Puhl, and Sean Constigan, "Emerging Security Challenges: Framing the Policy Context" GCSP Policy Paper 2013/5, Geneva Center for Security Policy, July 29, 2013, http://www.gcsp.ch/News-Knowledge/Publications/Emerging-Security-Challenges-Framing-the-Policy-Context; Pierrakakis et al., "3D Printing and Its Regulation Dynamics."

A. POLICY PITFALLS AND FAILED DETERRENCE

As demonstrated in the case-study section, much of the failure of current policy and regulatory efforts in the digital and technological realm is due to three primary factors. The first is that both national and international policy are still grounded in a Westphalian concept of law, designed for a nation-state system, not a system in which nation-states would be faced with borderless groups wielding new forms of power that enable them to compete at the state or regional level. The second factor is that the deterrent effect of these policies and laws is mitigated by the digital environment. Criminals and rogue actors make rational choices to commit illegal acts because they understand that these laws are ill suited to mete out punishment. This calculus has empowered individuals and non-state actors to push forward in areas where a nation-state may hesitate for fear of repercussions. But in the age of RLT, it is difficult if not impossible to punish an actor three time zones away for a digital or technological action that impacts an individual within US jurisdiction. Even basic counterproliferation efforts require months of paperwork and collaboration before they can move forward internationally.[163] How much more complex, then, will it be to coordinate effective deterrence in this new era of nonattribution and anonymizing tech? The third and final factor is that the current legal and regulatory framework from which most of the world operates lacks the flexibility to address the complexity of RLT coupled with human ingenuity. This system fails to incorporate how existing social orders react to the imposition of a legal system that may contradict the norms and rules they have established for themselves. Using existing law to cover new challenges instead of devising new laws that actually address the problem leads to failed, ineffective policy. Decentralization, anonymization, compliance without effect, the Streisand effect, and motivation crowding are all the end results of policy that fails to consider the nonlegal norms that already exist as part of the online and technological cultures.

[163] John Shiffman, *Operation Shakespeare: The True Story of an Elite International Sting* (New York: Simon & Schuster, 2014); Tuccille, "After Silk Road"; Soska and Christin, "Measuring the Longitudinal Evolution."

Dr. Colin Scott, a professor at the University College of Dublin School of Law, presents an alternative to this path. Instead of attempting to regulate at a distance, governments should seek first to understand the existing organization and social structures within the policy problem, because regardless of the implemented policy or the establishment of a new regulatory regime, these features will remain.[164]

> A more fruitful approach would be to seek to understand where the capacities lie within the existing regimes, and perhaps to strengthen those which appear to pull in the right direction and seek to inhibit those that pull the wrong way. In this way, the regulatory reform agenda has the potential to address issues of regulatory fragmentation in a manner that recognizes both the limits of government capacity and the potential of reconceptualizing regulation in other ways, for example that invoke non-state actors and alternative mechanisms to hierarchy.[165]

This approach encourages smart policy that incorporates existing cultural norms and mechanisms to ensure success, acceptance, and adherence. Truly knowing the perspectives of those who are to be regulated can help avoid conflict between rival normative orders that results in failure. This is not easy, and it requires time to identify and understand these mechanisms and how to utilize them to good effect. Policymakers and regulators will need to have patience, skill, and finesse to operate in the RLT environment, as well as a good deal of creativity and imagination.[166]

Deterrence is a continual challenge for both the world of technology and the digital environment. Until penalties can be effected in a timely manner, maintaining law and regulating actors will be problematic. Here the problem is certainly capacity. Nation-states simply don't have the ability to enact specific deterrence within these spaces using existing laws to good effect. A better option might be to seek opportunities for general

---

[164] Davis, Nacht, and Lehman, *Strategic Latency and World Power*; Roger Brownsword, "In the Year 2061: From Law to Technological Management," *Law, Innovation and Technology* 7, no. 1 (July 1, 2015): 1–51, doi: 10.1080/17579961.2015.1052642; Desai and Magliocca, "Patents, Meet Napster"; Dobson, *From Wassenaar to Mars*; *Economist*, "What is the Streisand Effect?"; Bryans, "Unlocked and Loaded"; Storch, "Down the Garden Path"; Colin Scott, "Regulating Everything" UCD Geary Institute Discussion Paper Series, February 26, 2008), 1–34.

[165] Brownsword, "In the Year 2061"; Colin Scott, "Regulating Everything."

[166] Davis, Nacht, and Lehman, *Strategic Latency and World Power*; Brownsword, "In the Year 2061"; Simon Roberts, "After Government? On Representing Law without the State," *Modern Law Review* 68, no. 1 (January 2005): 1–24.

deterrence, targeting potential crimes before they are committed by incorporating online norms that reinforce the desired end state. Other options, such as technology management, prevent the actors from making a negative choice; the technology or programming won't allow for it. But this too could be problematic, as sometimes radical actions are required to trigger much-needed change or to solve a new problem. This also brings up the question of personal freedoms versus the need for security. Technology management has the added danger of allowing those who control the technology to control the user. If these entities act in a self-interested way, much damage could be done. Figuring out how and where to draw the limits of regulation and even more importantly finding commonality between regulation and those being regulated will be critical to success. If regulation fails to understand the norms already in play, any instituted legal norms will be limited in effect and will serve to increase the complexity and danger of the problem set.[167]

B. MOVING FORWARD TO THE FUTURE: A SPECTRUM OF SOLUTIONS

In research this topic, it became clear very quickly that this was an important area in which not much work was being done. The reasons for this are as complex as the problem set itself, but the primary causes are that 1) nation-states have not recognized the level to which the world is changing around them or that power is being translated in new ways and 2) the speed of RLT development and the technical aspects make it difficult for those not in tune with these spaces to understand how radically and how fast this change is coming.[168]

The good news is that there is time to develop a viable response to deal with the challenges posed by RLT and to do so in a way that allows for innovation yet still protects state and international security. The following model is intended to be an initial

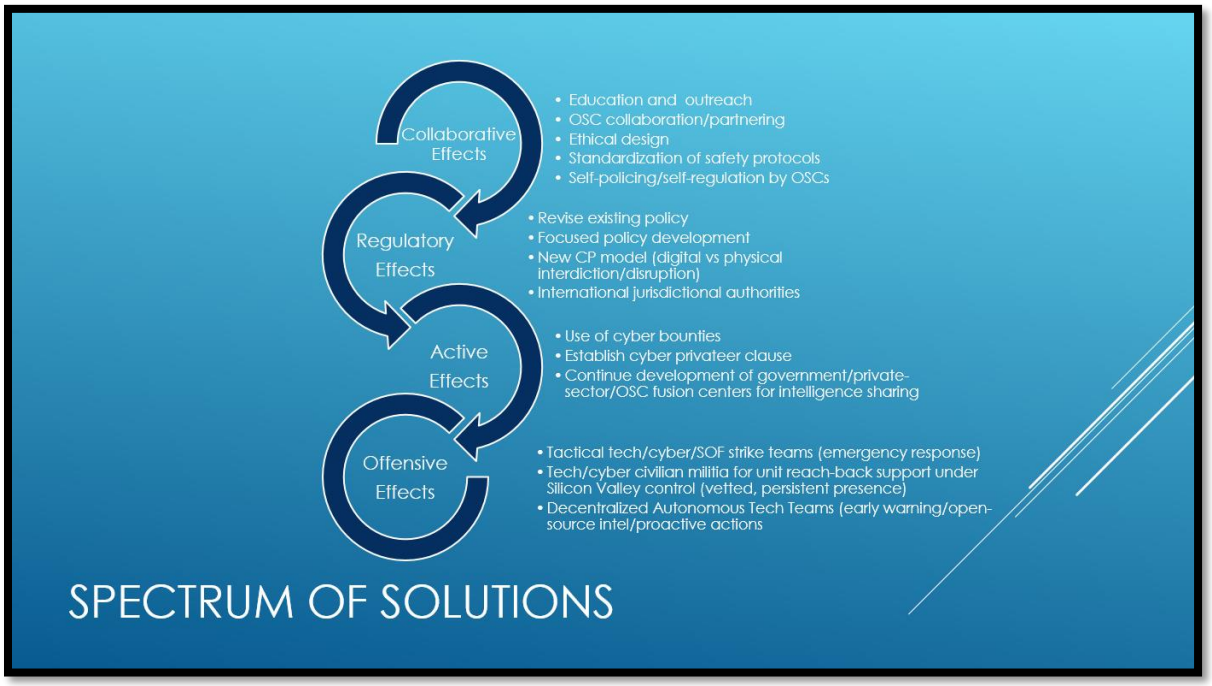
[167] Brownsword, "In the Year 2061"; Roger Grimes, "Why Internet Crime Goes Unpunished," *InfoWorld*, January 10, 2012, http://www.infoworld.com/article/2618598/cyber-crime/why-internet-crime-goes-unpunished.html; Laurence Martin, "The Determinants of Change: Deterrence and Technology," *Adelphi Papers* 20, no. 161 (1980): 9–19, doi: 10.1080/05679328008457371.

[168] Briggs and Shingles, "Exponentials"; Davis, Nacht, and Lehman, *Strategic Latency and World Power*; FitzGerald and Sayler, *Creative Disruption*; Pierrakakis et al., "3D Printing and Its Regulation Dynamics."

framework from which to build in this area. It is not all encompassing, and while it provides ample options for response, it is certainly not a final resolution. In fact, if this type of strategizing and response is done correctly, it should evolve with technology.

The model (shown below) denotes four portions of a spectrum, each of which contains specific action options. From top to bottom, the options move from benign proactive solutions to active or reactive offensive options during a crisis event. The intent is that by pursuing the options at the top, nation-states will avoid having to invoke the options at the bottom. The four areas on the spectrum are Collaborative Effects, Regulatory Effects, Active Effects (interdiction/preemption), and Offensive Effects (crisis/event response). Each of these areas is intertwined with the next, as they are all interdependent and necessary for an effective response.

Figure 3. Spectrum of Solutions



C. COLLABORATIVE EFFECTS

This entire process must start with education. Policymakers must understand the subtle nuances of specific technology and the underlying culture they are trying to

regulate. The first step in becoming well informed is to partner with those OSCs, both individuals and groups, at the leading edge of the RLT that exist today, as well as any that may arise in the future. These subject-matter experts can provide an accurate understanding of the risks and benefits and offer valuable insight into the types of policy and regulation that will or won't work. This must be a two-way collaborative process in which both parties become stakeholders and information sharing is open and transparent. Other collaborative options include encouraging ethical technological design which informs users on acceptable use and safety and encourages features within the existing cultures that promote similar values. Only in extreme cases should technological management efforts be pursued, as this will change the ability of an RLT to progress in specific ways and may result in unforeseen negative consequences that can increase problem-set complexity. Additional outreach is necessary to improve and repair relationships with isolated OSCs, such as DIY neurotechnology. It is critical that outreach to isolated groups send the right message, focusing on safety and security first while still guaranteeing the ability to innovate.[169]

Outreach to OSCs and the public should be done both in person and through appropriate digital means. Recent efforts by the FBI, US Department of Health, and US Department of State to collaborate with the DIY biohackers and amateur biotechnology communities have improved information sharing and created a culture of shared values. Development of a shared culture, especially where values, norms, and ethics are in sync, is critical to successful policymaking. OSCs not only provide the expertise and understanding policymakers need but they also function as ambassadors and liaisons to their communities. When government teams with OSC members, this also impacts their reputation and credibility with the community. Positive interactions mean the community will be more open to discussions and collaboration on smart policy that focuses on specific problem areas. This in turn limits the adoption of anonymizing behaviors, as the communities feel comfortable operating in the open; both parties have a shared trust and

[169] Charisius, Friebe, and Karberg, "Becoming Biohackers"; Dobson, *From Wassenaar to Mars*; Leibrand, "Working with the FDA"; Lempinen, "FBI, AAAS Collaborate."

set of expectations that work to prevent threat actors from exploiting expertise or group resources.[170]

Safety and standardization of RLT has already begun in several areas. Underwriters Laboratory (UL) is working on safety protocols for the 3D-printing industry to include specifics on operations and materials. DIYBio and its associates are also crafting a standardized set of safety and operating protocols that will be required for all individuals seeking to participate in this field. Efforts such as these should be encouraged and coupled with complimentary policy that builds on the strengths of existing self-regulation.[171]

D. REGULATORY EFFECTS

It is also necessary to revisit national and international counterproliferation, cyber, and technology policy. As highlighted earlier, much of existing policy falls short in these areas and in some cases results in more harm than good. The establishment of transnational policy to reduce jurisdictional conflict will also help close existing gaps that threat actors have been exploiting. With focused policy development that targets these gaps and also incorporates the expertise of subject-matter experts from the field, nations can begin to impact illicit actors in these spaces. But policy must also be accompanied by the tools and resources necessary to provide credible deterrence and consequences.

This is a preeminent feature of the developing challenges within existing counterproliferation models. RLT capabilities have demonstrated that disruption will become more difficult, especially as proliferators shift to the digital environment. While there are pathways to defeat proliferators and rogue actors, interdiction of materials and physical technology will only accomplish so much. Attempts to control technology and code, create back doors to defeat encryption, or restrict digital design should be avoided. Previous efforts using these methods have resulted in damaged relationships with OSCs, security issues that threat actors have successfully exploited, and increased anonymizing

[170] Charisius, Friebe, and Karberg, "Becoming Biohackers"; Dobson, *From Wassenaar to Mars*; Errera, "InfraGard Partnership for Protection Program"; Leibrand, "Working with the FDA"; Lempinen, "FBI, AAAS Collaborate."

[171] Dobson, *From Wassenaar to Mars*; Lempinen, "FBI, AAAS Collaborate."

behaviors. Collaborative effects can mitigate some of this damage by conducting outreach, sharing concerns, and rebuilding relationships with isolated OSCs to remove potential inroads for nefarious actors.[172]

Digital proliferation will have the biggest impact on types of weapons technology available to both states and non-state actors.[173] The production model for technology and weapons has reversed from one where the government could transition technology over to civilian use to one that starts with civilian development of technologies which are then transitioned over for government or military use. Civilians have access to technology immediately as it is released, which makes it incredibly hard to regulate. Dual-use digital technologies in particular will be a significant challenge, as current regulations are nearly impossible to enforce online without resulting in negative effects and proliferation of the information. These technologies will become available to an increasing number of actors, and intelligence signatures will be reduced by the use of anonymizing tools and dark networks. Nuclear, chemical, and biological weapons, missile production, and other types of operations will be harder to detect and discover and may occur at the non-state-actor level. This calls for a new counterproliferation model, one that is in part derived from the digital environment and that will require the addition of some new tools.

E. ACTIVE EFFECTS

The tools described in this section, while new to the government and policymakers, certainly are not new to the business world. They are highly effective and are used on a daily basis, including for gathering open-source intelligence. As proliferation goes digital, counterproliferation efforts must incorporate some of these same tools to track and proactively defeat threat actors. This will require the assistance of OSCs and the open-source intelligence that only they, as digital natives, can provide. One of the biggest barriers to the use of the tools in this section will be bureaucratic. These tools are unconventional, rely on others operating as private contractors, and require

[172] Bryans, "Unlocked and Loaded"; Cohn, "Nine Epic Failures"; Dobson, *From Wassenaar to Mars*; Doctorow, "Laws Restricting Tech"; Storch, "Down the Garden Path."

[173] Hallex, Matthew. "Digital Manufacturing and Missile Proliferation." Federation of American Scientists, May 21, 2013. http://fas.org/pir-pubs/digital-manufacturing-and-missile-proliferation/.

autonomy in execution and operation, all factors that typically make nation-states uncomfortable. Yet they are used globally by major corporations to stay ahead of competitors, to provide a view to the future, to avoid or neutralize threats, or to stay ahead of the next RLT's disruptions. Active Effects will require a paradigm shift in security operation and will require a significant amount of trust in and freedom of action for those involved.[174]

Active efforts best suited to this type of proactive general deterrence include the use of cyber bounties, posted contracts requesting specific information and a reward for that information. The FBI already does this when searching for information on cyber criminals, and it's a good start. Corporations such as Microsoft and United Airlines have "bug bounties" which request assistance from private contractors to help find dangerous holes in software or hardware that could be exploited. These bounties encourage individuals or small teams to participate. Other efforts utilize a stacked approach in which individuals can accept a bounty and then send out a call for information to their networks. If the information is located, the individual at the top of the network receives a certain percentage of the bounty and the individuals who found the information as well as those who referred them to the bounty are also rewarded.[175]

Another option to be considered is reinvigorating the privateer clause under the US Constitution to utilize cyber privateers. Nations in the past had privateers to safeguard state property or locate specific criminals; cyber privateers could serve the same purpose. An individual or team could accept a contract to recover stolen goods, locate a black market enterprise, or identify cyber criminals and locate them for pickup by authorities.

---

[174] Arquilla, "To Build a Network"; Arquilla, "New Rules of War"; Grant, "Silicon Offset"; Committee on Science, Security, and Prosperity. *Beyond "Fortress America": National Security Controls on Science and Technology in a Globalized World* (Washington, DC: National Academies, 2009).

[175] Jeffery Dastin, "United Airlines Awards Hackers Millions of Miles for Revealing Risks," *Reuters*, July 16, 2015, http://www.reuters.com/article/2015/07/16/us-cybersecurity-airmiles-idUSKCN0PQ0A320150716; Gregg Keizer, "Microsoft Waves More Security Pros into the Pool for $100K Bounties," *Computerworld*, November 5, 2013, 1–4; Rene Millman, "FBI Offers $4.2m in Bounties to Catch Cybercriminals," *SC Magazine*, July 3, 2015, 1–2; Jason Polancich, "Incentivized Cyber Defense: Creating Your Own Cyber 'Bounty' Program,'" *SecurityWeek*, June 26, 2015, http://www.securityweek.com/incentivized-cyber-defense-creating-your-own-cyber-bounty-program; Eric Schonfield, "How to Find Those Red Balloons," *TechCrunch*, December 5, 2009, http://techcrunch.com/2009/12/05/how-to-find-those-red-balloons.

In return, these individuals would receive a commission from the state (i.e., existing reward money, an amount agreed up front, or cryptocurrencies, bandwidth, or storage) and could also receive a percentage of the hardware or resources seized by authorities. The fulfillment of digital bounties that highlight grave threats to public safety, stop significant infrastructure attacks, or disrupt terrorism plots would give a proactive edge to US security. This would also enable the government to expand its capacity substantially at minimal extra cost, because the program would use funds and resources that already exist for reward programs. The establishment of a cyber-privateer clause would enable the government to use an additional set of tools providing temporary or long-term cyber assets to improve security and safety online. Cyber privateers would be a means of identifying and locating threat actors discreetly, disrupting the digital side of black market operations, and providing an extra level of cyber policing focused on threat-actor early warning and interdiction.[176]

The final necessary piece is to continue to grow and evolve the network of national and international fusion centers. These centers are the incubators for the future of policing and international intelligence. Collaboration between government, private sector, and OSCs is critical for success, as is the structure of each center and the network as a whole. Such organizations will be hybrids, exceptionally agile and able to bridge the gap between government and the private and public sectors. Currently a collaborative group of businesses, academics, and members of the IC working out of Lawrence Livermore National Laboratory are discussing how best to meet national requirements and what form an entity working toward that should take. Efforts such as these should be encouraged, and suggestions should be solicited on how the government can use lessons

[176] Arquilla, “To Build a Network”; Arquilla, “New Rules of War”; Grant, “Silicon Offset”; Dastin, “United Airlines Awards Hackers”; Keizer, “Microsoft Waves More Security”; Millman, “FBI Offers $4.2m in Bounties”; Polancich, “Incentivized Cyber Defense”; Schultz, Robert. "Countering Extremist Groups in Cyberspace: Applying Old Solutions to a New Problem." CTX 5, no. 4, November 1, 2015. https://globalecco.org/countering-extremist-groups-in-cyberspace-applying-old-solutions-to-a-new-problem-ltc-robert-schultz-us-army.

learned from Silicon Valley and elsewhere to leapfrog security and intelligence forward.[177]

F. OFFENSIVE EFFECTS

At the extreme end of the spectrum are offensive effects. These tools provide a rapid response capability to crisis, a capability that includes access to both RLT subject-matter expertise and technology-augmented forces that can respond, neutralize, and/or contain active threats. Like special operations forces, these teams will take time to grow, will not be mass producible, and will be most effective when focused long term on a specific region of the world. Due to the nature and capabilities of RLT, especially within the CBRN-E realm, a cadre of technology-specialized forces will need to be developed to form the core of tactical tech/cyber/SOF strike teams that will be 24/7 worldwide deployable. Much of this capability exists and is already regionally focused. The majority of the work will be on how to incorporate new tools into the mix, how to respond to an RLT-generated event, and how these teams should be structured. Another key feature is to ensure that these teams have interjurisdictional capabilities to conduct emergency response around the globe. When an incident occurs, nations must be willing to accept help from a trained response unit or have their own capability on hand. An RLT event is the responsibility of all, so in these cases, it is imperative that nations work together so the crisis does not become a regional or global threat.[178]

Special operations forces around the globe are best suited for such operations and are agile enough to incorporate new tools. Some options would be establishing a vetted network of dedicated digital natives around the globe to provide active support during a crisis, creating a civilian technology- and cyber-militia from the tech centers around the United States to be an online presence for special mission unit reach-back under the leadership of Silicon Valley, and to establish decentralized autonomous technology teams (DATT) to provide early warning and open-source intelligence, with the authority to

[177] Errera, "InfraGard Partnership for Protection Program"; Miller, "Public and Private Sector Partnerships"; Scott, "FBI's InfraGard Program"; Stone, "National Fusion Center Model"; Williams, "University Professor Helps FBI."

[178] Arquilla, "To Build a Network"; Arquilla, "New Rules of War"; Grant, "Silicon Offset."

conduct small-scale digital interdictions and disruptions to protect national security, public safety, or critical assets. The DATT must be allowed freedom to operate as fluidly as their technological competitors on the web. The capacity and expertise for tools and teams like these are available via OSC partners, bounties, or cyber privateers. By partnering with OSC members and creating agile networks that can keep pace with the networks spawning RLT, the United States will be able to keep current with the steep curve of exponential innovation. This will require a new level of transparency, a willingness to partner with outside entities (some of which are very different from the mainstream), and the ability for these units and entities to act autonomously the majority of the time to prevent developing or active threats from achieving a successful end state.

VI. CONCLUSIONS AND ADDITIONAL RESEARCH RECOMMENDATIONS

It is my hope that this thesis will serve as a basic primer to the risks and benefits of the technological revolution that is upon us as well as a cautionary tale for those charged with the difficult task of policy development, regulation and enforcement. RLT will produce unprecedented effects that will require ingenuity, thoughtfulness and an agility that does not come easily to government entities. It will also require those in positions of power to reassess established protocols and consider ways to expand the existing circle of trust to include influential OSCs in planning for the next generation of international security.

Technology may already hold some of the answers. The incorporation of ethical design into RLT as well as active engagement with key technology drivers will likely produce creative and effective solutions to limit potential threat uses. Technology licensing is another possible solution that may help to ensure the technologies most at risk of illicit use are used in a responsible, ethical manner. Biometrics, improved digital immersion by providing a more active online presence and education and training on RLT are all options that should be discussed and considered within the sphere of possible solutions.

The recipe for success however lies with the incorporation of OSC participants. The online culture has much to teach us and many of these groups are more than willing to collaborate to make the world a safer place for everyone. As I write this, the actions of OSCs taken in response to the ISIS Paris attacks bear witness to this truth. Social media outlets are being used to warn of danger, to find shelter, and to provide authorities with important information. Hacktivist groups are operating in overdrive to shut down ISIS accounts and provide law enforcement with critical planning intelligence gleaned from terrorist chats and posts. Self-policing efforts by Twitter and Telegram have deleted ISIS propaganda channels. This is the power of people at work in a million different ways and places and times to fight terrorism. This is the untapped capacity of people who want to improve global security. A billion sets of eyes around the globe are watching and

warning, helping nations to fight back and keep the public safe by leveraging RLT. Cyber bounties, cyber privateering and collaborative teaming to establish a permanent vetted cyber civilian militia for 24/7 reach back support are all options to increase capacity, agility and expertise at low or no cost.

A great deal of work remains. The spectrum of solutions is just a simple framework at this point, a skeleton that needs a great deal of fleshing out. This will require the work of unconventionally minded, imaginative individuals who aren't afraid to get their hands dirty by jumping in and doing science. Priority areas for research under the RLT umbrella include much needed deep dives on synthetic biology, neurotechnology, and additive manufacturing, as well as advanced robotics, nanotechnology, and advanced genomics. Serious work on understanding these technologies, their drivers and the culture behind them is critical to defining what deterrence will look like in the next five years. Works on the viability of collaborative efforts such as the FBI DIYBio outreach and Silicon Valley's use of cyber bounties will provide much needed data on the development of comprehensive collaborative plans enhanced by the capacity and expertise of OSCs. Finally, a study on how to best build capacity using nontraditional partners such as OSC groups is long overdue. The networks necessary to defeat malicious actor networks may already exist in these spaces, they just need to be identified. Hacktivists are not the only groups making a difference. Understanding how to team with these entities to achieve limited or long term goals will help to increase international security.

This is an interesting time to be alive, and RLT will make it more so. The RLT problem set will be challenging, but there are viable, inexpensive solutions that can promote awareness through education, cultural understanding, and partnering. Policy will be the lynchpin in this area. In a world where non-state actors are already flexing their muscles and challenging heads of state directly via social media, it is only a matter of time before these same groups leverage developing technologies to more serious purpose. The current nation-state system exists in part because conflict brought all nations together to seek a better solution. It is only a matter of time before one nation's technological or cyber concerns become a concern for other nations, and if this nation-state system is to

continue to function successfully, it is critical that world leaders recognize the need for interjurisdictional, transnational policy that is smart, global, and enforceable. This spectrum of solutions will hopefully provide a starting point from which to make that happen.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Agence France-Presse. “3D Printing Could Revolutionize War and Foreign Policy.” *Space Daily*, January 5, 2015. http://www.spacedaily.com/reports/How_3D_printing_could_revolutionise_war_and_foreign_policy_999.html.

Ahlberg, Liz. “Muscle-powered Bio-bots Walk on Command.” *University of Illinois News Bureau*, June 13, 2014. https://news.illinois.edu/news/14/0630biobots2_rashidbashir.html.

Albright, David. *Peddling Peril: How the Secret Nuclear Trade Arms America’s Enemies*. New York: Free, 2013.

Albright, David and Corey Hinderstein. “Uncovering the Nuclear Black Market: Working toward Closing Gaps in the International Nonproliferation Regime.” Paper prepared for the 45th Annual Meeting of the Institute for Nuclear Materials Management (INMM), Orlando, FL, July 2, 2004.

Albright, David and Andrea Stricker. “Preliminary Assessment of the JCPOA Procurement Channel: Regulation of Iran’s Future Nuclear and Civil Imports and Considerations for the Future.” Institute for Science and International Security, August 31, 2015.

Albright, David, Andrea Stricker, and Houston Wood. *Future World of Illicit Nuclear Trade: Mitigating the Threat*. Washingon, DC: Institute for Science and International Security. July 29, 2013.

Albright, David, Andrea Stricker, David Schnur, and Sarah Burkhard. “Additional Taiwan-Based Element of Iranian Military Goods Procurement Network Exposed.” Institute for Science and International Security. September 16, 2015.

Anderson, Chris. *Makers: The New Industrial Revolution*. New York: Crown Business, 2012.

Anonymous. “FBI Using Information from Anonymous to Help Find U.S. Central Command Hackers.” Anonymous Activism. Accessed January 29, 2015. http://anonhq.com/.

Arquilla, John. “The New Rules of War.” *Foreign Policy*, February 11, 2010. http://foreignpolicy.com/2010/02/11/the-new-rules-of-war/.

———. “To Build a Network.” *Prism* 5, no. 1 (September 2014): 22–33. http://www.ndu.edu/Portals/59/Documents/CCO/PRISMVol5No1.pdf.

Arquilla, John and David Ronfeldt. Networks and Netwars: The Future of Terror, Crime, and Militancy. Santa Monica, CA: RAND Corporation, 2001. http://www.rand.org/pubs/monograph_reports/MR1382.html.

Bajarin, Tim. "This Will Be the Most Disruptive Technology over the Next Five Years." *Time,* January 12, 2015. http://time.com/3663909/technology-disruptive-impact/.

Balinski, Brent. "The 3D Printing Boom Continues." *Manufacturers' Monthly*, May 15, 2015. http://www.manmonthly.com.au/Features/The-3D-printing-boom-continues.

Baltimore, David, Paul Berg, Michael Botchan, Dana Carroll, R. Alta Charo, George Church, Jacob E. Corn, George Q. Daley, Jennifer A. Doudna, Marsha Fenner, Henry T. Greely, Martin Jinek, G. Steve Martin, Edward Penhoet, Jennifer Puck, Samuel H. Sternberg, Jonathan S. Weissman, and Keith R. Yamamoto. "A Prudent Path Forward for Genomic Engineering and Germline Gene Modification." *Science* 348, no. 6230 (April 2015): 36–38. doi: 10.1126/science.aab1028.

Barnatt, Christopher. 3D Printing: The Next Industrial Revolution. CreateSpace Independent Publishing Platform, 2013.

Basiliere, Pete. "3D Printing Predictions for 2013." *www.3ders.org*, December 30, 2012. http://www.3ders.org/articles/20121229-3d-printing-predictions-for-2013.html.

Basulto, Dominic. "Why it Matters that the FDA Just Approved the First 3D-Printed Drug." *Washington Post,* August 11, 2015. https://www.washingtonpost.com/news/innovations/wp/2015/08/11/why-it-matters-that-the-fda-just-approved-the-first-3d-printed-drug/.

Bayliss, Kelly. "Gay Couple Beaten in Possible Hate Crime Attack: Police." *NBC 10 Philadelphia* video, 2:26. September 12, 2014. http://www.nbcphiladelphia.com/news/local/2-Gay-Men-Attacked-by-Group-Center-City-274964621.html.

Bellamy, Jill. "Treating the Unthinkable: Vaccine Development for Unknown Synthetic Viruses." *Biological Warfare Blog: Black Six,* May 19, 2014. http://bio-defencewarfareanalyst.blogspot.com/2014/05/treating-unthinkable-vaccine.html.

———. "DARPA's 7-Day Bio-Defence and the Future of Synthetic Vaccines." *Biological Warfare Blog: Black Six,* Janyary 4, 2015. http://bio-defencewarfareanalyst.blogspot.com/2015/01/darpas-7-day-bio-defence-and-future-of.html.

———. "Emerging Technologies: Lowering the Threshold for ISIS (Islamic State of Iraq and Syria) Mass Casualty Terrorism." *Biological Warfare Blog: Black Six*, July

31, 2015. http://bio-defencewarfareanalyst.blogspot.com/2015/07/emerging-technologies-lowering.html.

Bentham, Harry. "Virus: Rebutting the Fear of Synthetic Biology." Institute for Ethics and Emerging Technologies. May 13, 2014.

Biggs, John. "Solid Concepts Announces Another 3D-Printed Metal Gun." *TechCrunch*, October 27, 2014. http://techcrunch.com/2014/10/27/solid-concepts-announces-another-3d-printed-metal-gun/.

Bower, Joseph L., and Clayton M. Christensen. "Disruptive Technologies: Catching the Wave." *Harvard Business Review* 73, no. 1 (January-February 1995): 43–53.

Boyle, Rebecca. "How the First Crowdsourced Military Vehicle Can Remake the Future of Defense Manufacturing." Popular Science, June 30, 2011. http://www.popsci.com/cars/article/2011-06/how-first-crowdsourced-military-car-can-remake-future-defense-manufacturing.

Brafman, Ori, and Rod A. Beckstrom. *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*. New York: Penguin, 2006.

Briggs, Bill and Marcus Shingles. "Exponentials." *Deloitte University Press*, January 29, 2015. http://dupress.com/articles/tech-trends-2015-exponential-technologies/?id=us:2el:3dc:dup1012:eng:cons:tt15.

Bright, Peter. "HP's Spout PC is Like a Real Version of Ironman's JARVIS." *ARS Technica*, October 29, 2014. http://arstechnica.com/gadgets/2014/10/hps-sprout-pc-is-like-a-real-version-of-iron-mans-jarvis/.

Brodwin, Erin. "New Generation of Bio-Hackers Make DNA Misbehave." *Newsweek*, June 26, 2014. http://www.newsweek.com/2014/07/04/new-generation-bio-hackers-make-dna-misbehave-256322.html.

Brownstone, Sydney. "DNA Sanitizer Will Wipe Your Identity Off Everything You Touch." *Fast Company*, May 9, 2014. http://www.fastcoexist.com/3030150/dna-sanitizer-will-wipe-your-identity-off-everything-you-touch.

Brownsword, Roger. "In the Year 2061: From Law to Technological Management." *Law, Innovation and Technology* 7, no. 1 (July 2015): 1–51. doi: 10.1080/17579961.2015.1052642.

Bryans, Danton. "Unlocked and Loaded: Government Censorship of 3D-Printed Firearms and a Proposal for More Reasonable Regulation of 3D-Printed Goods." *Indiana Law Journal* 90, no. 2 (April 2015): 901–34.

Butler Millsaps, Bridget. “Autodesk Genetic Engineer Is Able to 3D Print Viruses, Soon to Attack Cancer Cells.” *3DPrint.com*, October 17, 2014. http://3dprint.com/19594/3d-printed-virus-fights-cancer/.

Camp, Jean, and Ken Lewis. “Code as Speech: A Discussion of Bernstein v. USDOJ, Karn v. USDOS, and Junger v Daley in Light of the U.S. Supreme Court’s Shift to Federalism.” *Ethics and Information Technology* 1, no. 2 (August 2001): 1–13.

Canton, James. *Future Smart: Managing the Game-Changing Trends that Will Transform Your World*. Boston: Da Capo, 2015.

Canton, James, Toby Redshaw, and Rudy Burger. “New Frontiers in Emerging and Disruptive Technology: Where to Look for Innovation and Competition - and Where Not to Look.” Center for Global Security Research, Lawrence Livermore National Laboratory. May 27, 2015.

Castro, Daniel. “Should Government Regulate Illicit Uses of 3D Printing?” Information Technology and Innovation Foundation, May 16, 2013. https://itif.org/publications/2013/05/16/should-government-regulate-illicit-uses-3d-printing.

Charisius, Hanno, Richard Friebe, and Sascha Karberg. “Becoming Biohackers: The Long Arm of the Law.” *BBC*, January 24, 2013. http://www.bbc.com/future/story/20130124-biohacking-fear-and-the-fbi.

Chatsko, Maxx. “5 Crazy Technologies made Possible by 3-D Bioprinting.” *Motley Fool*, November 12, 2013. http://www.fool.com/investing/general/2013/11/12/5-crazy-technologies-made-possible-by-3-d-bioprint.aspx.

Chopra, Samir, and Scott Dexter. “The Political Economy of Open Source.” *International Journal of Technology, Knowledge, and Society* 1, no. 1 (2005): 1–14.

Chowdhry, Amit. “What Can 3D Printing do? Here Are 6 Creative Examples.” *Forbes*, October 8, 2013. http://www.forbes.com/sites/amitchowdhry/2013/10/08/what-can-3d-printing-do-here-are-6-creative-examples/.

Christensen, Clayton. “Disruptive Innovation.” Clayton Christensen website. Accessed December 8, 2014. http://www.claytonchristensen.com/key-concepts/.

Clark, Liat. “Disarming Corruptor Distorts 3D Printing Files for Sharing of Banned Items.” *Wired UK*, November 5, 2013. http://www.wired.co.uk/news/archive/2013-11/05/disarming-corruptor.

Clark, Libby. “Jono Bacon: Open Source is Where Society Innovates.” *Linux.com*, October 14, 2014. https://www.linux.com/news/featured-blogs/200-libby-clark/791644-jono-bacon-open-source-is-where-society-innovates.

Cohen, Daniel, Matthew Sargeant, and Ken Somers. “3-D Printing Takes Shape.” *McKinsey & Company*, January 2014.

Cohn, Cindy. “Nine Epic Failures of Regulating Cryptography.” *Deeplinks* (Blog). Electronic Frontier Foundation, September 26, 2014. https://www.eff.org/deeplinks/2014/09/nine-epic-failures-regulating-cryptography.

Collins, Katie. “Meet the Biologist Hacking 3D Printed Cancer-Fighting Viruses.” *Wired UK*, October 16 2014.

Columbus, Louis. “2015 Roundup of 3D Printing Market Forecasts and Estimates.” *Forbes*, March 31, 2015.

Committee on Science, Security, and Prosperity. *Beyond “Fortress America”: National Security Controls on Science and Technology in a Globalized World*. Washington, DC: National Academies, 2009.

Computer Sciences Corporation Leading Edge Forum. *3D Printing and the Future of Manufacturing*. Falls Church, VA: Computer Sciences Corporation, 2012. http://assets1.csc.com/innovation/downloads/LEF_20123DPrinting.pdf.

Cook, James. “How a Hacker Gang Literally Saved Christmas for Video Game Players Everywhere.” *Business Insider*, December 16, 2014. http://www.businessinsider.com/lizard-squad-hack-playstation-and-xbox-2014-12?r=UK&IR=T.

Coughlan, Shane, ed. *Research on Open Innovation: A Collection of Papers on Open Innovation from Leading Researchers in the Field*. N.p: OpenForum Europe, 2014.

Craig, James, Michael Eubanks, and Gary Warner. “CKN-3: Operation Trident Breach - Lessons Learned from FBI Global Cyber Crime Arrests.” Proceedings of the FOSE Conference and Exposition, Washington, D.C., July 19–21, 2011.

Cuthbertson, Anthony. “Anonymous Lists 9,200 Twitter Accounts Linked to Islamic State After Hacktivist Collaboration.” *International Business Times*, March 16, 2015. http://www.ibtimes.co.uk/anonymous-lists-9200-twitter-accounts-linked-islamic-state-after-hacktivist-collaboration-1492035.

———. “Anonymous Affiliate GhostSec Thwarts ISIS Terror Plots in New York and Tunisia.” *International Business Times*, July 22, 2015. http://www.ibtimes.co.uk/anonymous-affiliate-ghostsec-thwarts-isis-terror-plots-new-york-tunisia-1512031.

Damron, Regan W., and William Busch. “Game Changing Developments in the Proliferation of Small Arms and Light Weapons, Part 2 of 2: Additive Manufacturing.” EUCOM J2: EUCOM ECJ2 Strategy Division, Deep Futures, 2013.

Damron, Regan W., and Brian G. Henke. “Game-changing Developments in the Proliferation of Small Arms and Light Weapons, Part 1 of 2: Anonymizing Technologies.” EUCOM J2: EUCOM ECJ2 Strategy Division, Deep Futures. February 5, 2013.

Dastin, Jeffery. “United Airlines Awards Hackers Millions of Miles for Revealing Risks.” *Reuters*, July 16, 2015. http://www.reuters.com/article/2015/07/16/us-cybersecurity-airmiles-idUSKCN0PQ0A320150716.

Davis, Zachary, Michael Nacht, and Ronald Lehman, eds. *Strategic Latency and World Power: How Technology Is Changing Our Concepts of Security*. Livermore, CA: Center for Global Security Research, Lawrence Livermore National Laboratory, 2014.

Department of Justice. “Former Owner of Defense Contracting Businesses Pleads Guilty to Illegally Exporting Military Blueprints to India without a License.” April 1, 2015. http://www.justice.gov/opa/pr/former-owner-defense-contracting-businesses-pleads-guilty-illegally-exporting-military.

———. “Summary of Major U.S. Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases” (January 2008 to the present: updated January 23, 2015). August 2015. http://www.justice.gov/sites/default/files/nsd/pages/attachments/2015/01/23/export-case-list-201501.pdf.

Department of Homeland Security. “ICS-CERT Monitor Spring 2013.” 2013.

———. “ICS-CERT Monitor 2014 Fiscal Report.” 2015.

———. “ICS-CERT Monitor 2015.” 2015.

Department of State. “Controls Tangible/Intangible.” Accessed January 8, 2015. http://www.state.gov/strategictrade/practices/c43180.htm.

Desai, Devan R., and Gerard N. Magliocca. “Patents, Meet Napster: 3D Printing and the Digitization of Things.” *Georgetown Law Journal* 102, no. 6 (April 2014): 1691–720.

Dewey-Hagborg, Heather. “Stranger Visions.” Accessed May 7, 2015. http://deweyhagborg.com/strangervisions/about.html.

Dewey-Hagborg, Heather, Surya Mattu, Tega Brain, Josiah Zaynor, Aurelia Moser, Brian Holmes, Fei Liu, Ignacio Larrain, and Jeremy Gruber. “DIY Guides to DNA Spoofing.” biononymous.me. Accessed October 7, 2015. http://biononymous.me/diy-guides/.

DiBona, Chris, Sam Ockman, and Mark Stone, eds. *Open Sources: Voices from the Open Source Revolution*. Sebastopol, CA: O’Reilly, 1999.

Digital Malaysia. “What is MSC Malaysia?” Accessed May 7, 2015. http://www.mscmalaysia.my/what_is_msc_malaysia.

Dobson, Michael. *From Wassenaar to Mars: Open Source Hardware, U.S. Export Controls, and Avoiding Missteps in the Maker Movement*. N.p.: Kelley Drye, 2015. http://www.kelleydrye.com/publications/articles/1927/_res/id=Files/index=0/wassenaar_whitepaper_v3.pdf.

Doctorow, Cory. “How Laws Restricting Tech Actually Expose Us to Greater Harm.” *Wired*, December 24, 2014. http://www.wired.com/2014/12/government-computer-security/.

Dodrill, Tara. “Breaking: Government Claims Control of Wiki Weapons Project.” *Off the Grid News*. Accessed August 3, 2015. http://www.offthegridnews.com/self-defense/guns-ammo/breaking-government-claims-control-of-wiki-weapons-project/.

Dodziuk, Helena. “What’s New in 3D Printing?” *ChemViews*, February 12, 2014. doi: 10.1002/chemv.201300064.

Doll, Steve. “Hovership: 3D Printed Racing Drone.” *Make:* 44, March 2015.

Dreazen, Yochi. “The Next Arab-Israeli War Will Be Fought with Drones.” *Diplomat*, March 26 2014.

Drzik, John. “Error on Terror: Controlling Emerging Technology.” *CNBC*, January 15, 2015. http://www.cnbc.com/id/102340274.

Dugdale, Addy. “Philadelphia is the First City to Ban 3-D-Printed Guns.” *Fast Company*, November 25, 2013. http://www.fastcompany.com/3022195/philadelphia-is-the-first-city-to-ban-3-d-printed-guns.

Economist. “The Economist Explains: What is the Streisand Effect?” April 15, 2013. http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-what-streisand-effect.

Electronic Frontier Foundation. “RIAA v. the People: Fiver Years Later.” September 30, 2008. https://www.eff.org/wp/riaa-v-people-five-years-later.

———. “Electronic Frontier Foundation.” Accessed July 27, 2015. https://www.eff.org/issues.

Errera, Amylynn. “InfraGard Partnership for Protection Program Overview.” Federal Bureau of Investigation, Washington Field Office, 2014.

Estes, Adam Clarke. “3D-Printed Guns Are Only Getting Better and Scarier.” *Gizmodo*, January 6, 2015. http://gizmodo.com/3d-printed-guns-are-only-getting-better-and-scarier-1677747439.

Eunjung Cha, Ariana. “Glowing Plant Project on Kickstarter Sparks Debate about Regulation of DNA Modification.” *Washington Post*, October 3, 2013. https://www.washingtonpost.com/national/health-science/glowing-plant-project-on-kickstarter-sparks-debate-about-regulation-of-dna-modification/2013/10/03/e01db276-1c78-11e3-82ef-a059e54c49d0_story.html.

Federal Bureau of Investigation. “Amerithrax or Anthrax Investigation.” https://www.fbi.gov/about-us/history/famous-cases/anthrax-amerithrax. Accessed March 5, 2015. https://www.fbi.gov/about-us/history/famous-cases/anthrax-amerithrax.

Federal Bureau of Investigation, Internet Crime Complaint Center. 2011 Internet Crime Report. N.p.: Internet Crime Complaint Center, 2011.

———. 2014 Internet Crime Report. N.p.: Internet Crime Complaint Center, 2014.

Fell, Jason. “How Steve Jobs Saved Apple.” *Entrepreneur*, October 27, 2011. http://www.entrepreneur.com/article/220604.

FitzGerald, Ben, and Kelley Sayler. *Creative Disruption: Technology, Strategy and the Future of the Global Defense Industry*. Washington, DC: Center for a New American Security, 2014.

Fox-Brewster, Thomas. “Hundreds of Wind Turbines and Solar Systems Wide Open to Easy Exploits.” *Forbes*, June 12, 2015. http://www.forbes.com/sites/thomasbrewster/2015/06/12/hacking-wind-solar-systems-is-easy/.

Franzoni, Chiara, and Henry Sauermann. “Crowd Science: The Organization of Scientific Research in Open Collaborative Projects.” *Research Policy* 43, no. 1 (2014): 1–20. doi: 10.2139/ssrn.2167538.

Freedonia Group. “Industry Study Report by the Freedonia Group: Global Demand for 3D Printing to Rise Over 20% Annually through 2017.” 3D Printer Technology Forum. 2014.

Geere, Duncan. “Kickstarter Bans Project Creators from Giving Away Genetically-Modified Organisms.” *Verge*, August 2, 2013.

Germain, Jack M. “Next on the Open Source Horizon: 3D Printing.” *LinuxInsider*, May 28, 2014. http://www.linuxinsider.com/story/80519.html.

Ghost Security. “Ghost Security.” Accessed August 15 2015. http://www.ghostsec.org/.

Gibbs, Donna, and Kerri-Lee Krause, eds. *Cyberlines 2.0: Languages and Cultures of the Internet*. Albert Park, Australia: James Nicholas, 2006.

Gibson, Daniel G., John I. Glass, Carole Lartigue, Vladimir N. Noskov, Ray-Yuan Chuang, Mikkel A. Algire, Gwynedd A. Benders, Michael G. Montague, Li Ma, Monzia M. Moodie, Chuck Merryman, Sanjay Vashee, Radha Krishnakumar, Nacyra Assad-Garcia, Cynthia Andrews-Pfannkoch, Evgeniya A. Denisova, Lei Young, Zhi-Qing Qi, Thomas H. Segall-Shapiro, Christopher H. Calvey, Prashanth P. Parmar, Clyde A. Hutchison III, Hamilton O. Smith, and J. Craig Venter. "Creation of a Bacterial Cell Controlled by a Chemically Synthesized Genome." *Science* 329, no. 5987 (July 2010): 52–56. doi: 10.1126/science.1190719.

Gilbert, David. "FBI Using Information from Anonymous to Help Find US Central Command Hackers." *International Business Times*, January 20, 2015.

Gillard, Nick. "Dual-use Traders: The Real WMD Threat in Southeast Asia?" *Diplomat*, January 22, 2015.

Gilpin, Lindsey and Jason Hiner. "New 3D Bioprinter to Reproduce Human Organs, Change the Face of Healthcare: The Inside Story." TechRepublic, August 1, 2014.

Giordano, James, Maren Holmes, and Paul Bracken. "Constraints on Exploiting Emerging S&T for Military Purposes: Is the Sky Falling." Center for Global Security Research, Lawrence Livermore National Laboratory, May 27, 2015.

Giordano, James, Anvita Kulkarni, and James Farwell. "Deliver Us from Evil? The Temptation, Realties, and Neuroethico-legal Issues of Employing Assessment Neurotechnologies in Public Safety Initiatives." *Theoretical Medicine and Bioethics* 35, no. 1 (February 2014): 73–89. doi: 10.1007/s11017-014-9278-4.

Global Industry Analysts, Inc. "Global Synthetic Biology Market: Trends, Drivers, and Projections." Accessed May, 7, 2015. http://www.strategyr.com/MarketResearch/Synthetic_Biology_Market_Trends.asp.

Goldin, Melissa. Chinese Company Builds Houses Quickly with 3D Printing. *Mashable*, April 29, 2014. http://mashable.com/2014/04/28/3d-printing-houses-china/.

Goldman, Emily O., and Leo J. Blanken. "The Economic Foundations of Military Power." In *Guns and Butter: The Political Economy of International Security*, edited by Peter Dombroski, 35–54. Boulder, CO: Lynne Rienner, 2005.

Goldstein, Phil. "LightSquared Could Target First Responders, Transport and Energy Industries with New Service." *FierceWireless*, April 8, 2015.

http://www.fiercewireless.com/story/lightsquared-could-target-first-responders-transport-and-energy-industries/2015-04-08.

———. "LightSquared Hires Advisers to Help Overcome GPS Industry Concerns." *FierceWireless*, June 30, 2015. http://www.fiercewireless.com/story/lightsquared-hires-advisers-help-overcome-gps-industry-concerns/2015-06-30.

Goodman, Marc. "Crime Has Gone High-Tech, and the Law Can't Keep Up," *Wired*, March 21, 2015.

———. *Future Crimes: Everything is Connected, Everyone is Vulnerable, and What We Can Do about It*. New York: Doubleday, 2015.

Goodman, Marc, and Parag Khanna. "The Power of Moore's Law in a World of Geotechnology." *National Interest* no. 123 (January-February 2013): 64–73.

Goodwin, Bruce T. "Additive Manufacturing and High-Performance Computing: A Disruptive Latent Technology." Presentation at the meeting of the American Physical Society, San Antonio, Texas, March 5, 2015.

Grant, Rebecca. "The Silicon Offset." *Air Force Magazine*, March 2015.

Greenberg, Andy. "Feds Tighten Restrictions on 3D Printed Gun Files Online." *Wired*, June 11, 2015.

Grimes, Roger. "Why Internet Crime Goes Unpunished." *InfoWorld*, January 10, 2012. http://www.infoworld.com/article/2618598/cyber-crime/why-internet-crime-goes-unpunished.html.

Grunewald, Scott. "Cambrian Genomics 3D Printing DNA — Sets its Sights on Space Dinosaurs." *3D Printing Industry*, April 10, 2014. http://3dprintingindustry.com/2014/04/10/cambrian-genomics-3d-printing-dna/.

Grushkin, Daniel. "Artist Turns DNA from Chewed Gum into Sculptures." *Popular Science*, January 1, 2015.

Gustafson, Krystina. "Lowe's Brings 3-D Printing to Home Improvement." April 29, 2015. http://www.cnbc.com/id/102627784.

Gutowski, Stephen. "Pioneer of 3D Printed Guns Explains Why He's Suing the State Department." *Washington Free Beacon*, July 8, 2015.

Hagel, John, III, John Seely Brown, Tamara Samoylova, and Michael Lui. "From Exponential Technologies to Exponential Innovation: Report 2 of the 2013 Shift Index Series." *Deloitte University Press*, October 4, 2013. http://dupress.com/articles/from-exponential-technologies-to-exponential-innovation/.

Hallex, Matthew. “Digital Manufacturing and Missile Proliferation.” Federation of American Scientists, May 21, 2013. http://fas.org/pir-pubs/digital-manufacturing-and-missile-proliferation/.

Hashem, Ali. “Assassinated Hezbollah Leader Key to Technology, Drone Operations.” *Al Monitor,* December 4, 2013. http://www.al-monitor.com/pulse/originals/2013/12/hezbollah-assassinated-hashem.html.

Hatcher, Jordan S. “Of Otaku and Fansubs: A Critical Look at Anime Online in Light of Current Issues of Copyright Law.” *SCRIPT-ed* 2, no. 4 (December 2005): 545–71. doi: 10.2966/scrip.020405.514.

Hayase, Nozomi. “Blockchain Revolution: Open Source Democracy for the 99%.” *openDemocracy UK*, August 4, 2014. https://www.opendemocracy.net/ourkingdom/nozomi-hayase/blockchain-revolution-open-source-democracy-for-99.

Heimans, Jeremy. “What New Power Looks Like.” TED video, 15:08. June 2014. https://www.ted.com/talks/jeremy_heimans_what_new_power_looks_like?language=en.

Herd, Grame P., Detlef Puhl, and Sean Constigan. “Emerging Security Challenges: Framing the Policy Context” GCSP Policy Paper 2013/5. Geneva Center for Security Policy, July 29, 2013. http://www.gcsp.ch/News-Knowledge/Publications/Emerging-Security-Challenges-Framing-the-Policy-Context.

Herman, Arthur. “Obama vs. GPS.” *National Review*, September 21, 2011.

Hessel, Andrew, Marc Goodman, and Steven Kotler. “Hacking the President’s DNA.” *Atlantic*, November 2012.

Hicks, Jennifer. “3D Printed Virus to Attack Cancer Cells.” *Forbes,* October 29, 2014.

Hipolite, Whitney. “Chinese Company 3D Prints a Full-Size Working Car For Just $1770.” *3DPrint.com,* March 25, 2015. http://3dprint.com/53532/chinese-3d-printed-car/.

Homeland Security News Wire. “Day of Synthetic Pathogens-based Bioterrorism Nears.” September 16, 2010. http://www.homelandsecuritynewswire.com/day-synthetic-pathogens-based-bioterrorism-nears.

Hughes, Eric. “A Cypherpunk’s Manifesto.” Activism.net. March 9, 1993. http://www.activism.net/cypherpunk/manifesto.html.

Hull, Chuck. “Pioneer in Stereolithography.” *SPIE Professional*, January 15, 2013.

Inside Edition. "Social Media Sleuth Helps Catch Police Chief's Daughter Charged in Gay Bashing." Video. September 26, 2014. http://www.insideedition.com/headlines/8996-social-media-sleuth-helps-catch-police-chiefs-daughter-charged-in-gay-bashing.

Johnson, Julian J. "Print, Lock, and Load: 3-D Printers, Creation of Guns, and the Potential Threat to Fourth Amendment Rights." *University of Illinois Journal of Law, Technology & Policy* 2 (2013): 337–61.

Jontz, Sandra. "Critical Infrastructure Is Cyberterrorism's Next Likely Target." *Signal*, March 2015, 18–21.

Kahn, Richard, and Douglas Kellner. "Internet Subcultures and Oppositional Politics." Post-subcultures Reader (2003): 299–314. https://pages.gseis.ucla.edu/faculty/kellner/essays/internetsubculturesoppositionalpolitics.pdf.

———. "New Media and Internet Activism: From the 'Battle of Seattle' to Blogging." *New Media & Society* 6, no. 1 (February 2004): 87–95. doi: 10.1177/1461444804039908.

Kampani, Gaurav. "WMD Diffusion in Asia: Heading Toward Disaster?" In *Strategic Asia 2004–05: Confronting Terrorism in the Pursuit of Power*, edited by Ashley J. Tellis and Michael Willis, 379–425. Seattle: National Bureau of Asian Research, 2004.

Kassenova, Togzhan. "1540 in Practice: Challenges and Opportunities for Southeast Asia." Stanley Foundation, May 2011.

———. "A Regional Approach to WMD Nonproliferation in the Asia-Pacific." *Carnegie Endowment for International Peace*, August 14, 2012.

Keizer, Gregg. "Microsoft Waves More Security Pros into the Pool for $100K Bounties." *Computerworld*, November 5, 2013.

Kershner, Isabel. "Israel Shoots down Drone Possibly Sent by Hezbollah." *New York Times*, April 25, 2013.

Kotler, Stephen. "Vice Wars: How 3-D Printing Will Revolutionize Crime." *Forbes*, July 13 2012. http://www.forbes.com/sites/stevenkotler/2012/07/31/the-democratization-of-vice-the-impact-of-exponential-technology-on-illicit-trades-and-organized-crime/.

Krassenstein, Brian. "The Moore's Law of 3D Printing… Yes It Does Exist, and Could Have Staggering Implications." *3DPrint.com*, June 28, 2014. http://3dprint.com/7543/3d-printing-moores-law/.

Krassenstein, Eddie. “Forecast 3D to Show off This Racecar, Featuring 45 3D Printed Parts at RAPID Event next Week.” *3DPrint.com,* May 13, 2015. http://3dprint.com/65093/forcast-3d-printed-racecar/.

———. “German Company Aims to Sell 3D Printed Drugs & A 3D Drug Printer.” *3DPrint.com,* August 10, 2015. http://3dprint.com/87977/3d-printed-drugs-2/.

Krebs, Brian. “DHS Blasts Reports of Illinois Water Station Hack.” *Krebs on Security* (blog), November 22, 2011. http://krebsonsecurity.com/2011/11/dhs-blasts-reports-of-illinois-water-station-hack/.

Lawrence, Jon. “3D Printing: Legal and Regulatory Issues.” *Electronic Frontiers Australia,* August 8, 2013. https://www.efa.org.au/2013/08/08/3d-printing-issues.

Lawson, Stephen. “LightSquared Vs. GPS Raises Big Spectrum Issues.” *PCWorld,* July 25, 2011.

Leibrand, Scott. “How and Why We Are Working with the FDA: Background and a Brief Summary of the Recent Meeting with the FDA about the Nightscout Project.” *DIYPS.org,* October 12, 2014. http://diyps.org/2014/10/12/how-and-why-we-are-working-with-the-fda-background-and-a-brief-summary-of-the-recent-meeting-with-the-fda-about-the-nightscout-project/.

Lempinen, Edward W. “FBI, AAAS Collaborate on Ambitious Outreach to Biotech Researchers and DIY Biologists.” *American Association for the Advancement of Science*, April 1, 2011. http://www.aaas.org/news/fbi-aaas-collaborate-ambitious-outreach-biotech-researchers-and-diy-biologists.

Levy, Steven. “Crypto Rebels.” *Wired,* January 2, 1993.

———. “Cypher Wars: Pretty Good Privacy Gets Pretty Legal.” *Wired,* November 2, 1994.

Linstone, Harold A., and Murray Turoff, eds. *The Delphi Method: Techniques and Applications*. Information Systems Department, New Jersey Institute of Technology, 2002. http://is.njit.edu/pubs/delphibook/.

Local Motors. “Local Motors Rally Fighter.” Accessed May 5, 2015. https://shop.localmotors.com/products/local-motors-rally-fighter.

loldhs pr0f. “City of South Houston SCADA Vulnerabilities.” *Grid: A Digital Frontier* (blog). November 18, 2011. http://pastebin.com/Wx90LLum.

Love, Dylan. “Why Microsoft and Sony Couldn’t Stop Lizard Squad Attack Despite Warnings.” *International Business Times,* December 30, 2014.

Lucibella, Michael. “Manufacturing Revolution May Mean Trouble for National Security.” *APS Physics* 24, no. 4 (April 2015).

Manyika, James, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson, and Alex Marrs. “Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy.” *McKinsey & Company*, May 2013. http://www.mckinsey.com/insights/business_technology/disruptive_technologies.

Marks, Paul. “3D Printing and Augmented Reality to Help Model Drugs.” *NewScientist*, October 18, 2011. http://www.newscientist.com/blogs/onepercent/2011/10/3d-printed-viruses-meet-their.html.

Martin, Laurence “The Determinants of Change: Deterrence and Technology,” *Adelphi Papers* 20, no. 161 (1980): 9–19. doi: 10.1080/05679328008457371.

Materialise. “3D Print Design Show NYC.” Meckler Media. Accessed May 5, 2015. http://www.3dprintdesignshow.com/.

Mattox, John Mark. “Additive Manufacturing and its Implications for Military Ethics.” *Journal of Military Ethics* 12, no. 3 (2013): 225–34. doi: 10.1080/15027570.2013.847534.

McIntosh, James. “‘Night Vision Eyedrops’ Improve Vision up to 50 Meters in Dark.” *Medical News Today*, March 30, 2015. http://discovermagazine.com/2009/sep/04-forget-goggles-chlorophyll-eye-drops-give-night-vision.

McLaughlin, W. “The Use of the Internet for Political Action by Non-State Dissident Actors in the Middle East.” *First Monday* 8, no. 11 (November 2003). doi: 10.5210/fm.v8i11.1096.

McNulty, Conner M., Neyla Arnas, and Thomas Campbell. “Toward the Printed World: Additive Manufacturing and Implications for National Security.” *Defense Horizons*, no. 73 (September 2012): 1–16.

Mearian, Lucas. “U.S. State Department Moves to Block 3D-Printed Gun Plans Online.” *ComputerWorld*, July 7, 2015.

Meyer, Robinson. “3-D Printed Drugs Are Here.” *Atlantic*, August 19, 2015.

Milkert, Heidi. “Hong Kong Terrorists Caught with 3D Printer, Perhaps Looking to Modify Airsoft Guns.” *3DPrint.com*, June 26, 2015. http://3dprint.com/76737/3d-printer-terrorists/.

Miller, Corinne. “The Video Game Industry and Video Game Culture Dichotomy: Reconciling Gaming Culture Norms with the Anti-Circumvention Measures of the DMCA.” *Texas Intellectual Property Law Journal* 16, no. 1 (spring 2008): 453–83.

Miller, Matthew. “Formalizing Fusion Center Public and Private Sector Partnerships, A Practical Model” San Diego Law Enforcement Coordination Center & San Diego InfraGard Member Alliance White Paper. March 2015.

Millman, Rene. “FBI Offers $4.2m in Bounties to Catch Cybercriminals.” *SC Magazine*, July 3, 2015.

Milward, H. Brinton, and Jörg Raab. “Dark Networks as Organizational Problems: Elements of a Theory.” *International Public Management Journal* 9, no. 3 (2006): 333–60.

Mistbreaker News. “Summarized: The 3D-printing Medical Achievements of the Past Year.” January 3 2015. http://www.mistbreaker.com/medicine-biotech/summarized-3d-printing-medical-achievements-past-year/.

Molitch-Hou, Michael. “US Military Turns to Hollywood’s Legacy Effects to 3D Print Iron Man Suit.” *3D Printing Industry*, July 9, 2014. http://3dprintingindustry.com/2014/07/09/us-military-turns-hollywoods-legacy-effects-3d-print-iron-man-suit/.

———. “5 Pairs of 3D Printed Shoes You’ll See at Milan Design Week 2015.” *3D Printing Industry*, April 14, 2015. http://3dprintingindustry.com/2015/04/14/5-pairs-of-3d-printed-shoes-youll-see-at-milan-design-week-2015/.

Muphy, Simon, and Russell Myers. “How Mail on Sunday ‘Printed’ First Plastic Gun in UK Using a 3D Printer and Then Took It on Board Eurostar without Being Stopped in Security Scandal.” *Daily Mail*, May 11, 2013.

Musil, Steven. “FCC Suspends LightSquared Waiver over GPS Interference.” *CNET*, February 14, 2012.

Nakashima, Ellen. “Water-Pump Failure in Illinois Wasn’t Cyberattack after All.” *Washington Post*, November 25, 2011.

Nandikotkur, Geetha. “Assessing Singapore’s Cyber Manifesto.” infoRisk Today, January 23, 2015. http://www.inforisktoday.com/assessing-singapores-cyber-manifesto-a-7829/op-1.

Nguyen, Nicole. “The Evolution of the Cell Phone—How Far It’s Come!” *ReadWrite*, July 4, 2014. http://readwrite.com/2014/07/04/cell-phone-evolution-popsugar.

Nuclear Threat Initiative. “Asia Could See Growing WMD Threat, Expert Warns.” August 21, 2008. http://www.nti.org/gsn/article/asia-could-see-growing-wmd-threat-expert-warns/.

Paganini, Pierluigi. “ICS-CERT MONITOR Report States Most Critical Infrastructure Attacks Involve APTs.” *Security Affairs* (blog), March 16, 2015.

http://securityaffairs.co/wordpress/34936/cyber-crime/ics-cert-monitor-report-apt.html.

Paul, Ian. "'Disarming Corruptor' Disguises 3D Printing Designs to Fight the Man." *PCWorld*, November 5, 2013. http://www.pcworld.com/article/2060822/disarming-corruptor-disguises-3d-printing-designs-to-fight-the-man.html.

Phoenix, Chris. "Administrative Options for Molecular Manufacturing." Center for Responsible Nanotechnology. Accessed May 5, 2015. http://crnano.org/administration.htm.

Pierce, Terry C. *Warfighting and Disruptive Technologies: Disguising Innovation*. Abingdon, UK: Frank Cass, 2004.

Pierrakakis, Kyriakos, Miltiadis Kandias, Charitini D. Gritzali, and Dimitris Gritzalis. "3D Printing and its Regulation Dynamics: The World in Front of a Paradigm Shift." Paper presented at the Proceedings of the 6th International Conference on Information Law and Ethics, Thessaloniki, Greece, May 30–31, 2014.

Polancich, Jason. "Incentivized Cyber Defense: Creating Your Own Cyber 'Bounty' Program." *SecurityWeek*, June 26, 2015. http://www.securityweek.com/incentivized-cyber-defense-creating-your-own-cyber-bounty-program.

Pollack, Andrew. "A Dream of Trees Aglow at Night." *New York Times*, May 7, 2013.

Powell, Alison. "Emerging Issues in Internet Regulation: The Unstable Role of Wikileaks and Cyber-Vigilantism." In *Research Handbook on Internet Governance*, edited by Ian Brown. Northampton, MA: Edward Elgar, 2012.

Proffitt, Brian. "How Open Source Hardware Is Driving the 3D-Printing Industry." *ReadWrite*, July 3, 2012. http://readwrite.com/2012/07/03/how-open-source-hardware-is-driving-the-3d-printing-industry.

Pugh, John. "Vaccines Built on A 3D Printer." *PSFK*, November 11, 2012. http://www.psfk.com/2012/11/build-vaccines-3d-printer.html.

Randerson, James. "Did Anyone Order Smallpox?" *Guardian*, June 23, 2006.

Rapoza, Kenneth. "The World's 10 Busiest Ports." *Forbes*, November 11, 2014.

Raymond, Eric. *The Cathedral & the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. 3rd ed. Sebastopol, CA: O'Reilly, 2001.

Redshaw, Toby. "The Big Bifurcation Battle – CIO Winners and Losers in 2015 and how to Land on the Winning Side." *Sand Hill*, January 27, 2015. http://sandhill.com/article/the-big-bifurcation-battle-cio-winners-and-losers-in-2015-and-how-to-land-on-the-winning-side/.

———. “The Internet of Things Isn’t: A Thought Leadership Briefing on Profiting in the Next-Gen Internet.” *Sand Hill*, June 22, 2015. http://sandhill.com/exec-briefing/the-internet-of-things-isnt-a-thought-leadership-briefing-on-profiting-in-the-next-gen-internet/.

———. “The Internet of Things is Not the Next Big Story for the Internet.” *Sand Hill*, June 24, 2015. http://sandhill.com/article/the-internet-of-things-is-not-the-next-big-story-for-the-internet/.

RFSID. “Lizard Squad: Two Bot Thugs.” *Recorded Future*, January 19, 2015. https://www.recordedfuture.com/lizard-squad-analysis/.

Rheingold, Howard. *Smart Mobs: The Next Social Revolution*. Cambridge, MA: Perseus Publishing, 2003.

Rheingold, Howard. “The Virtual Community.” Accessed August, 25 2015. http://www.rheingold.com/vc/book/.

Roberts, Simon Arthur. “After Government? On Representing Law without the State.” *Modern Law Review* 68, no. 1 (January 2005): 1–24.

Ross, Philip. “‘Printing’ Alien Life? Geneticist Craig Venter Says 3D Printers Could Recreate Martian DNA on Earth.” *International Business Times*, October 7, 2013.

Russel, Daniel R. “Remarks by Daniel R. Russel Assistant Secretary, Bureau of East Asian and Pacific Affairs on the Trans-Pacific Partnership for the National Bureau of Asian Research Roundtable.” U.S. Department of State, April 1, 2015.

Russia Today, “First Ban in the Country: 3D-printed Guns Now Illegal in Philadelphia.” November 25, 2013. https://www.rt.com/usa/philly-gun-ban-johnson-280/.

Samadi, David. “You Can Now 3D Print Prescription Drugs.” *Observer*, August 12, 2015. http://observer.com/2015/08/print-your-prescription-3d-technology-modernizes-medicine/.

Samuelson, Pamela. “Three Reactions to MGM v. Grokster.” *Michigan Telecommunications and Technology Law Review* 13 (2006): 177–96.

Schonfield, Eric. “How to Find Those Red Balloons.” *TechCrunch*, December 5, 2009. http://techcrunch.com/2009/12/05/how-to-find-those-red-balloons.

Schultz, Robert. "Countering Extremist Groups in Cyberspace: Applying Old Solutions to a New Problem." CTX 5, no. 4, November 1, 2015. https://globalecco.org/countering-extremist-groups-in-cyberspace-applying-old-solutions-to-a-new-problem-ltc-robert-schultz-us-army.

Scott, Colin. “Regulating Everything” UCD Geary Institute Discussion Paper Series. February 26, 2008.

Scott, Parker. “The FBI’s InfraGard Program.” Presentation. InfraGard San Diego Members Alliance, July 20, 2012. http://www.infragardsd.org/docs/isd-ppt.pdf.

Scutti, Susan. “FDA Approves First Ever 3D-Printed Epilepsy Drug from Aprecia; Set to Create More Central Nervous System Pills.” *Medical Daily*, August 4, 2015.

Shea, Virginia. “Netiquette.” Albion.com. Accessed August 25, 2015. http://www.albion.com/netiquette/.

Shiffman, John. *Operation Shakespeare: The True Story of an Elite International Sting*. New York: Simon & Schuster, 2014.

Shirky, Clay. “How the Internet Will (One Day) Transform Government.” TED video, 18:32. June 2012. https://www.ted.com/talks/clay_shirky_how_the_internet_will_one_day_transform_government?language=en.

Shmigelsky, Geoffrey. “Exponential Technology.” Think Exponential. Accessed May 6, 2015. http://thinkexponential.com/invest/exponential-technology/.

Sifry, Micah L. “The Rise of Open-Source Politics.” *Nation*, November 4, 2004. http://www.thenation.com/article/rise-open-source-politics/.

Silver, David. “Introducing Cyberculture.” Resource Center for Cyberculture Studies, University of San Francisco. Last modified December 10, 2009. http://rccs.usfca.edu/intro.asp.

Siryoti, Daniel. “Iran Admits Hezbollah’s Drone over Israel used Iranian Technology.” *Associated Press*, October 14, 2012. http://www.israelhayom.com/site/newsletter_article.php?id=6075.

Soska, Kyle and Nicolas Christin. “Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem.” Paper presented at the Proceedings of the 24th USENIX Security Symposium, Washington, D.C., August 12–14, 2015.

Steele, Robert David. *The Open-Source Everything Manifesto; Transparency, Truth & Trust*. Berkeley, CA: Evolver, 2012.

Stone, Adam. “National Fusion Center Model Is Emerging.” *Emergency Management*, January 23, 2015. http://www.emergencymgmt.com/safety/National-Fusion-Center-Model-Is-Emerging.html.

Stone, Brad. “Steve Jobs: The Return, 1997–2011.” *Bloomberg Businessweek*, October 6, 2011. http://www.bloomberg.com/bw/magazine/the-return-19972011-10062011.html.

Storch, Joseph C. “3-D Printing Your Way down the Garden Path: 3-D Printers, the Copyrightization of Patents, and a Method for Manufacturers to Avoid the Entertainment Industry’s Fate.” *New York University Journal of Intellectual Property & Entertainment Law* 34, no. 2 (spring 2014): 249–309.

Stott, Rory. “A Giant 3D Printer Builds Ten Houses in One Day.” *Huffington Post*, September 2, 2014. http://www.huffingtonpost.com/2014/09/08/3d-printed-houses_n_5773408.html.

Szondy, David. “ORNL Unveils 3D-Printed Shelby Cobra in Detroit.” *Gizmag*, January 13, 2015. http://www.gizmag.com/3d-printed-shelby-cobra-ornl/35575/.

———. “GE Fires up Fully 3D-Printed Jet Engine.” *Gizmag*, May 13, 2015. http://www.gizmag.com/ge-fires-up-all-3d-printed-jet-einge/37448/.

Thomas, Jim. “Kickstopper Letter to ‘Glowing Plants’ Project.” *ETC Group*, May 7, 2013. http://www.etcgroup.org/content/kickstopper-letter-glowing-plants-project.

Thompson, Derek. “The 10 Fastest-Growing (and Fastest-Declining) Cities in the World.” *Atlantic*, January 19, 2012.

Thorpe, Nick. “Hungary Internet Tax Cancelled after Mass Protests.” *BBC News*, October, 31, 2014. http://www.bbc.com/news/world-europe-29846285?print=true.

Timmer, John. “New DNA Construct Can Set Off a “Mutagenic Chain Reaction.”” *Ars Technica*, March 23, 2015.

Trowbridge, Alexander. “Evolution of the Phone: From the First Call to the Next Frontier.” *CBS News*, December 6, 2014. http://www.cbsnews.com/news/evolution-of-the-phone-from-the-first-call-to-the-next-frontier/.

Tuccille, J. D. “After Silk Road, Online Illicit Marketplaces for Drugs and Weapons Grow, with More to Come.” *reason.com*, August 25, 2015. https://reason.com/archives/2015/08/25/after-silk-road-online-illicit-marketpla.

Tufekci, Zeynep, and Christopher Wilson. “Social Media and the Decision to Participate in Political Protest: Observations from Tahrir Square.” *Journal of Communication* 62, no. 2 (April 2012): 363–79. doi: 10.1111/j.1460-2466.2012.01629.x.

Turner, Samantha. “The Evolution of Cell Phones.” Presentation. March 2012. http://community.mis.temple.edu/mis3538c2/files/2012/03/cellphoneinfographic.jpg.

Turton, William. “Lizard Squad’s Xbox Live, PSN Attacks Were a ‘Marketing Scheme’ for New DDoS Service.” *Daily Dot*, December 30, 2014. http://www.dailydot.com/crime/lizard-squad-lizard-stresser-ddos-service-psn-xbox-live-sony-microsoft/.

Ulanoff, Lance. “World’s First 3D Printed Car Took Years to Design, but Only 44 Hours to Print.” *Mashable*, September 16, 2014. http://mashable.com/2014/09/16/first-3d-printed-car/.

United Nations Environment Programme. “COP 12 Decision XII/24 New and Emerging Issues: Synthetic Biology.” 12th meeting of the Conference of the Parties to the Convention on Biological Diversity, Pyeongchang, Korea, October 6–17, 2014.

University of California, Santa Cruz. “UCSC Ebola Genome Portal.” UCSC Genome Informatics Group. Accessed May 6, 2015. https://genome.ucsc.edu/ebolaPortal/.

Van Zuylen-Wood, Simon. “Philly Becomes First City to Ban 3-D Gun Printing.” *Philadelphia*, November 21, 2013.

Vandita. “Anonymous Takes down ISIS Websites, Confirms Leaked Government Documents were real.” Anonymous HQ. Accessed January 29, 2015. http://anonhq.com/anonymous-takes-isis-websites-confirms-leaked-government-documents-real/.

Venter, J. Craig. “First Self-replicating Synthetic Bacterial Cell.” J. Craig Venter Institute. Accessed May 7, 2015. http://www.jcvi.org/cms/research/projects/first-self-replicating-synthetic-bacterial-cell/overview/.

Vezina, Kenrick. “Culture Wars Threaten Synthetic Biology’s Future: Debate on Open Source Versus Closed Door.” *Genetic Literacy Project*. May 9, 2014. http://www.geneticliteracyproject.org/2014/05/09/culture-wars-threaten-synthetic-biologys-future-debate-on-open-source-versus-closed-door/.

Virus Pathogen Research. “Ebolavirus.” Accessed May 7, 2015. http://www.viprbrc.org/brc/home.spg?decorator=filo_ebola.

Wainwright, Oliver. “The First 3D-Printed Pill Opens up a World of Downloadable Medicine.” *Guardian*, August 5, 2015.

Waldefogel, Joel. “Digitization, Copyright, and New Media Products: Evidence from Recorded Music.” Presentation. Global Governance Programme, December 14–15, 2012. http://globalgovernanceprogramme.eui.eu/wp-content/uploads/2013/01/Joel-Waldefogel.pdf.

Walther, Gerald. “Printing Insecurity? The Security Implications of 3D-Printing of Weapons.” *Science and Engineering Ethics* (December 2014): 1–11. doi: 10.1007/s11948-014-9617-x.

Warrick, Joby. “FBI Investigation of 2001 Anthrax Attacks Concluded; U.S. Releases Details.” *Washington Post*, February 20, 2010.

Whitwam, Ryan. “US State Department Begins the Nearly Impossible Task of Banning 3D Printed Guns Online.” *ExtremeTech*, July 8, 2015. http://www.extremetech.com/extreme/209461-us-state-department-begins-the-nearly-impossible-task-of-banning-3d-printed-guns-online.

Williams, Brian. “University Professor Helps FBI Crack $70 Million Cybercrime Ring.” *Rock Center NBC News*, March 21, 2012. http://rockcenter.nbcnews.com/_news/2012/03/21/10792287-university-professor-helps-fbi-crack-70-million-cybercrime-ring.

Williams, Phil. “The Nature of Drug-Trafficking Networks.” *Current History* 97, no. 618 (April 1998): 154–59.

Williams, Rob. “Home Depot Sets up MakerBot 3D Printer Kiosks in 12 Stores.” *HotHardware*, July 14, 2014.

Wilson, Cody. “Ghost Gunner.” Defense Distributed. Accessed May 5, 2015, https://ghostgunner.net/.

Wohlers, Terry and Tim Caffrey. “Wohlers Report 2015: 3D Printing and Additive Manufacturing State of the Industry Annual Worldwide Progress Report.” Wohlers Associates. 2015.

Woollaston, Victoria. “Privacy Spray Promises to Remove All Traces of DNA from Surfaces - but Could It Be Used to Commit Crimes without Getting Caught?” *Daily Mail*, May 7, 2014.

Worstall, Tim. “Both GE and Rolls Royce are to use 3D Printing to make Jet Engines and Violate Engineering's Prime Commandment.” Forbes (2 December 2013, 2013): 1-2.

Worstall, Tim. “How Cute, Philadelphia Passes Law Banning 3D Gun Printing.” *Forbes*, November 25, 2013.

Xanatos, David, and Ekliptor. “EMULE: A Decade of File Sharing Innovations.” TorrentFreak. May 13, 2012. https://torrentfreak.com/emule-a-decade-of-file-sharing-innovations-120513/.

York, Jillian. “EFF Signs Joint Coalition Letter Urging Companies to be Proactive on Export Regulations.” *Electronic Frontier Foundation*, June 27, 2012. https://www.eff.org/deeplinks/2012/06/eff-signs-joint-coalition-letter-urging-companies-be-proactive-export-regulations.

You, Edward H. “FBI Perspective: Addressing Synthetic Biology and Biosecurity.” Presentation. Presidential Commission for the Study of Bioethical Issues, Washington, D.C., July 9, 2010.

Young, H. Peyton. *Individual Strategy and Social Structure: An Evolutionary Theory of Institutions*. Princeton, NJ: Princeton Univ, Press, 2001.

Zegart, Amy B. "September 11 and the Adaptation Failure of U.S. Intelligence Agencies." *International Security* 29, no.4 (spring 2005): 78–111.

———. *Spying Blind: The CIA, the FBI, and the Origins of 9/11*. Princeton, NJ: Princeton Univ. Press, 2009.

———. "The Coming Revolution of Drone Warfare." *Wall Street Journal*, March 18, 2015. http://www.wsj.com/articles/amy-zegart-the-coming-revolution-of-drone-warfare-1426720364.

Zetter, Kim. "DHS Issued False 'Water Pump Hack' Report; Called it a 'Success.'" *Wired*, February 10, 2012.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California